Alma Mater Studiorum - Università di Bologna

in cotutela con MYKOLO ROMERIO UNIVERSITETAS - MYKOLAS ROMERIS UNIVERSITY

DOTTORATO DI RICERCA IN

LAW, SCIENCE AND TECHNOLOGY

Ciclo 35

Settore Concorsuale: 12/H3 - FILOSOFIA DEL DIRITTO

Settore Scientifico Disciplinare: IUS/20 - FILOSOFIA DEL DIRITTO

INTERNET OF THINGS: LEGAL LIABILITY OF IOE DEVICES IN THE HOME

Presentata da: Francesca Gennari

Coordinatore Dottorato

Monica Palmirani

Supervisore

MINDAUGAS KIŠKIS

Co-Supervisore

Giovanni Sartor

Co-supervisore

Michele Graziadei
Università degli Studi di Torino

Esame finale anno 2023

Acknowledgement

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie ITN EJD grant agreement No 814177

Abstract

This thesis is about the smart home, a connected ambience that will help consumers to live a more environmentally sustainable life and will help vulnerable categories of consumers to live a more autonomous life, thanks to the pervasive use of the Internet of Things (IoT) technology. In particular, civil liability for the malfunctioning of the smart home is the filter through which the research is carried out. I analyse whether the actual legal liability rules are ready or not to adapt to this new connected environment, such as the IoT-powered smart home. Through careful mapping of the technical and legal state of the art, the thesis argues that the EU rules on product liability contained in the Product Liability Directive (PLD) will apply consistently to these objects. This holds true even if at the time of the drafting of the thesis, the proposal on the update of the PLD had not been published yet. Through the analysis of past PLD cases, new American products liability case-law on domestic IoT objects and the latest legal scholarship's contributions and policy inputs it was possible to anticipate some of the contents of the newly published EU PLD Update proposal.

Aurimui, draugui mano kelionės

ir daugelių kitų dalykų.

To Aurimas, my companion of travels

and of many other things

Table of Contents

Introduction 1

Chapter I – Methodology 12

1. Introduction 12
2. The main features of the research 12
3. The question(s) addressed in the research 14
4. Exclusions from the research field 15
5. Provisional answer, social significance of the research and objectives 16
6. Definitions 17

Chapter II - State of the Art part I: the IoT technology and the smart home 21

1. The state of the art 21
2. History of the IoT and struggles for a definition 22
3. The IoT structure 25
   - 3.1. The technological side: sensors 26
   - 3.2. The technological side: actuators 29
   - 3.3. The technological side: the gateway 30
   - 3.4. The technological side: the cloud 30
4. The smart home and the IoT paradigm 31
   - 4.1. Is the smart home still to arrive? 32
   - 4.2. Why the smart home is not yet here to stay 36
5. Functional taxonomies for the IoT in the home 41
   - 5.1. The novelty criterion 41
   - 5.2. The autonomy criterion 42
   - 5.3. The EU Commission classification of Consumer IoT 43
   - 5.4. Mixed functions of domestic IoT objects 44
6. Future technological perspectives 45
   - 6.1. Fog and Edge computing 45
   - 6.2. Distributed Ledger technologies and Blockchain for the home 47
   - 6.3. The new Green IoT (GIoT) 48

Chapter III: State of the Art part II - EU law and the IoEd objects of the smart home 50

1. Introduction 50
2. Legislative documents 51

2.1. Data laws and the IoT: an introduction 51
2.2. New and old EU consumer and contract law 61
2.2.1. New technologies and EU consumer law 62
2.2.2. Analogue application and progressive adaptation 66
I. The adaptation of the already existent EU Consumer law to the digital revolution 66
II. The New Approach and the New Legislative Framework Acts 69
3. Platform regulation and the IoT 75
3.1. The E-commerce Directive and the proposed Digital Services Act (DSA) 75
3.2. The Digital Markets Act (DMA) 77
4. More technical policy and legislative documents 80
4.1. The EECC, NIS and NIS 2: what they mean for the home IoT 80
5. The long path to AI (and its liability) regulation: consequences for domestic IoT objects. 84
Chapter IV: Liability in the EU and in the smart home 96
1. Liability and the smart home: past rationales and new meanings 96
1.1. The “traditional” functions and features of private law liability 97
1.1.1. The general functions of liability 97
1.1.2. The different features of EU private law liability and their degree of harmonization 98
I. Extra-contractual/Tort liability 99
II. Strict Liability- Objective and quasi objective-strict liability 104
III. Contractual liability 106
IV. Pre-contractual liability 109
1.2. Liability: risk and innovation 110
1.3. Liability: a balance between different actors 111
1.4. Liability: an enhancer of trust in IoT technology for the home 115
1.5. Liability in a home that changes: how perceptions of the home environment have changed and their impact on liability 116
2. Liability in EU private law and the smart home 122
2.1. The EU criteria for competence: the principle of conferral and the principle of subsidiarity 122
2.2. Is Article 114 TFEU (harmonization) and the single market clause sufficient to establish liability for new technologies in general? ... 125
2.3. The Charter for Digital Rights and a progressive path towards a more Constitution-oriented legal integration of new technologies 130
3. Product Liability for the home IoT: which possible constitutional scenarios? 132
Chapter V: Towards an updated PLD for the domestic IoEd objects ... 134

1. Introduction 134
1.1. The PLD: history and legal models 135
1.1.1. European product liability models before the EU PLD 139
1.1.2. EU PLD: the US model and EU harmonization 141
2. The implementation of the PLD: a quantitative and qualitative study based on CJEU case law 142
2.1. First quantitative and qualitative analysis of EU PLD-related cases: number and types of cases per Member State. 158
2.2. Second quantitative and qualitative analysis: the EU PLD's most challenged articles 163
3. The future PLD and its interaction with other legislative and policy documents. 170
3.1.1. Future Article 2 PLD 171
3.1.2. Future Article 3 PLD 174
3.1.3. Future Article 4 PLD 177
3.1.4. Future Article 6 PLD 178
3.1.5. Future Article 7 PLD 180
3.1.6. Future Article 9 PLD 182
3.1.7. Future Article 11 PLD 187
3.1.8. Future Article 13 PLD 188
4. Preliminary conclusions 190
Chapter VI: IoE home devices in the US. Theory and cases 191
1. Introduction 191
2. The US model: past and current trends with new technologies 192
2.1. A concise evolution of the US products liability theories 192
2.1.1. A certain kind of negligence: probability considerations and the Learned Hand formula 194
2.1.2. The "attack" on privity: from the implied merchantability warranty to the Uniform Commercial Code 195
2.1.3. 1963: The strict liability doctrine and its influence on the Restatement Second of Torts 199
2.1.4. New defects under the Restatement Third of Torts, and products liability to the present day. 201
2.2. US priorities in technology regulation: platforms, AI and the IoT 204
2.3. The home IoT and American legal scholarship 212
3. Case law on consumer IoT devices in the US 216
3.1. Security devices for the home 218
3.1.1. FTC cases 218
I. TRENDnet 220
II. Vizio 221
III. D-Link 222
IV. Tapplock 224
V. Comparison with EU law 226
3.1.2. Judicial case: Onity 226
I. Comparison with EU law 231
3.2. Toys and children's devices 231

3.2.1. VTech Data Breach Litigation 232
3.2.2. Archer-Hayes v. Toytalk, INC. 235
3.2.3. A comparison between Archer-Hays and V-Tech and EU law 236
3.3. Medical devices and IoT with medical functions 237
3.3.1. The Therac-25 Case. An ante litteram IoT case 238
3.3.2. The St Jude Medical LLC cases 239
I. American pre-emption and the St. Jude Medical LLC cases: Freed III, Mellott, Guinn and Ross 239
II. Comparison with EU law: deciding which liability for IoT with medical and consumer functions 246
3.4. Connected cars 248
3.4.1. Comparison with EU law 253
4. Some preliminary conclusions 255
Conclusions 259
1. Introduction 259
2. Systematic/organisational results 259
3. Analytical results 262
4. Creative results 265
5. Conclusive remarks 268
6. Table of results 270
Latest Developments 277
1. The AI Civil Liability Proposal (AILP) 278
2. The PLD Update (PLDU) 283
Bibliography 297
1. Articles, books, policy briefs and other documents 297
2. EU legal acts (proposed and enacted) 317
3. Conseil de l'Europe 322
4. US Planned and Enacted Bills, Restatements and Policy Documents 322
5. Cases 323
5.1. EU 323
5.2. Austria 327
5.3. France 327
5.4. Italy 327
5.5. UK 328
5.6. US 328
5.6.1. FTC orders and decisions 329
Personal acknowledgments 331

Most Frequently Used Abbreviations

AIA: (proposed) AI Act

ALI: American Law Institute

CJEU: Court of Justice of the European Union

DA: (proposed) Data Act

DCDS: Directive on distribution of Digital Content and supply of Digital Services

DGA: Digital Governance Act Regulation

DMA: Digital Markets Act

DSA: Digital Services Act

EG: Expert Group on Liability and New Technologies- New Technologies Formation

ELI: European Law Institute

EU: European Union

FDA: Food and Drug Administration

FFDR: Free Flow of Data Regulation

FTC: Federal Trade Commission (US)

GDPR: General Data Protection Regulation

IoE: Internet of Everything

IoT: Internet of Things. IoT and IoTs could also be used to indicate IoT objects

MDA: Medical Devices Amendments Act 1976 (US)

MDD: Medical Devices Directive

MDR: Medical Devices Regulation

MS: Member State/s

NB: Notified Body/ies

PLD: Product Liability Directive

SDG: Directive on Certain Aspects Concerning Contracts for the the Sale of Goods, including goods with digital elements

SDO: Standard Developing Organisation/s

SSO: Standard Setting Organisation/s

US: United States of America

Introduction

This thesis is about the smart home, namely a connected ambience that will help consumers to live a more environmentally sustainable life and will help vulnerable categories of consumers to live a more autonomous life, thanks to the pervasive use of the Internet of Things (IoT) technology. In particular, civil liability for the malfunctioning of the smart home is the filter through which this research is carried out. The fact of whether the actual legal liability rules are ready or not to adapt to this new type of connected environment, such as the IoT-powered smart home, will be investigated.

Needless to say, it is challenging to write a thesis on something that does not actually exist as such yet. The perfectly automated and connected environment, which was dreamt about from the 30s to the 70s, from Europe to the US, and known as "the intelligent - or smart – home" is still a dream. As of today, our homes are not fully autonomous environments. Despite this, the home we live in is probably the place where we use our smart-phones and our voice assistants, such as Google Home, Alexa or Siri, most of the time, or where we relax or exercise in front of a smart television. Briefly, these are smart objects, and they allow us to always be connected with people outside the home or inside it. Smart-phones and voice assistants are not the only smart objects that can be found in homes today. Indeed, the domestic IoT object is a booming market[1]. As a consequence, there seems to be an ever-growing number of smart appliances, from smart locks to smart lights, from smart washing machines to smart fridges and smart toys. Despite all these elements, an *ad hoc* regulation or directive in the EU with a comprehensive framework for these objects is not in place for the moment. As well as our own homes, EU law is transforming and starting to regulate these phenomena (IoT objects and smart homes) in a gradual, incremental way. However, this way of proceeding does not enhance consumers' trust in this new technology, as they do not know if they can rely on effective legal remedies, while they are increasingly aware of the power personal data give to the producers of these objects. In the next paragraphs, I will outline the main contents of each of the chapters of the thesis to introduce the reader to my work.

Chapter I is about methodology. In order to carry out this research, it is useful to do a summary list of challenges as a preliminary step to understand the methodology employed. The first challenge was that the subject matter was in constant evolution. In the space of three years - the timeframe of my PhD - things have changed consistently every four to six months, as far as the technical and legal state of the art were concerned. This can be stimulating but it also reduces the chances to find literature and, most importantly, judicial cases that can give a more practical angle to the thesis. Cases are also important as they are powerful proof to demonstrate theoretical assessment of the law. Moreover, they also let other and new problems emerge, which might have escaped a first *ex ante* assessment of legal and policy acts. The second challenge was the time

[1] Martin Armstrong, "The market for smart home devices is expected to boom over the next 5 years," *World Economic Forum with the collaboration of Statista*, April 29, 2022, https://www.weforum.org/agenda/2022/04/homes-smart-tech-market/.

constraint, which is actually a consequence of the ever-growing body of the state of the art. In fact, to have a complete understanding of how a new legislative initiative or policy might impact on the topic requires time. Often, time was not sufficient to allow existing legal and technical structures to consolidate before writing about them. To meet the challenge, I periodically updated and reviewed the chapters on the state of the art (Chapters II and III) until 31 August 2022[2]. Furthermore, to better analyse the legal issues, it was necessary to narrow down the subject to EU private law rules, meaning legislative acts and legal developments concerning consumers and contracts (hence businesses). Nevertheless, before doing that, I decided to try to explain the IoT technology that underpins smart homes in an accessible way. By following this process of progressively narrowing down the topic, the research ended up by focusing on the EU model of product liability in two separate chapters. In particular I investigated how the Product Liability Directive (PLD) will be impacted by the IoT for home technology (Chapter V). The choice of focusing on the PLD is also dictated by other factors. Firstly, it is one of the parts of the EU *consumer acquis* that it is left aside by the modernisation brought by the EU Commission Digital Strategy. Its updating process has been stalling for years and this has given scholars the possibility to suggest different theories on how to modify it in order to also adapt it to IoT technology[3]. The liveliness of the debate over the PLD update increased over recent months, hence it was an occasion to join it. This forecasting exercise was actually useful and interesting as I found some of the policy insights written at the end of Chapter V were included in the Product Liability Update[4].

The third challenge involved venturing into the study and survey of IoT technology architecture and how it functions. This was necessary in order to give an explanation of how this technology works and to find the ways in which this technology conflicts with EU private law. In addition to that, IoT has its own features which will have an impact on future liability rules, hence they need to be understood well. This technological focus was done by trying to give an exact and concise explanation of the technology for people with mostly a legal background.

The fourth challenge was to integrate a comparative legal analysis into the research. Comparative legal methods are valuable tools that compare and contrast the differences and the similarities between two or more legal systems, by taking into account the different sources of legal rules (legal formants) and by also adding history and sociology notions to understand the evolution of legal concepts and ideas. However, the comparative effort with focus on liability did not turn into a comparison of the 27 different EU legal models. Three years would not have sufficed for just one researcher to cover even half the systems. In Chapter V, I therefore decided to briefly describe the main features of the product liability systems of some countries (such as France, Germany, Spain, Denmark and the UK) whose PLD implementation was evaluated by the CJEU. Nevertheless, the true comparative effort took place in Chapter VI. The focus of

[2] However, for the most relevant legal and policy changes that took place after 31st August 2022, I have written a brief Appendix called “Latest Developments”. Its focus will be the AI extra-contractual liability directive and the Product Liability Directive Update proposals. The references to these documents could be found in the Appendix “Latest Developments” part of the thesis.

[3] A more detailed explanation of this can be found in Chapters III and IV

[4] See Appendix, Latest Developments.

this chapter was about the US legal model of product liability and how well it adapted to new technologies such as IoT. There were two methodological reasons for taking the US system as a reference. The first one was that IoT technology was developed there, hence the legal system might have had an indirect influence on it. The second one was the availability of several cases on domestic IoT objects concerning product liability, which were difficult to find at the EU level. The fifth methodological challenge was trying to use sociological insights in order to foresee the future evolution of the smart home and how to connect it better with environment protection, as I tried to do in chapter IV.

The second part of this chapter focuses instead on the definitions that will be important throughout the thesis. Specifically, the list of definitions in this part includes the Internet of Everything (IoE), the Internet of Things, and the smart home meanings that were employed throughout the thesis. In particular, one of the hypotheses is that the IoE would be present whenever there will be a completely connected environment and the connection with humans will be seamless, hence it is a concept that is still not applicable to my research because that does not still exist today. However, even by using the term of IoT throughout the thesis, there is an element of future "all-connectedness" implied, which is an aspect typical of the IoE. This is done in order to provide legal solutions that are mindful of the rights and expectations of human beings which the IoE will encompass fully, unlike the present IoT. Some definitions such as the ones concerning data and data processing are the ones of already passed or proposed EU legal acts. There will be occasions to discuss them critically in subsequent parts of the thesis. Other definitions, such as the definition of the IoT, are not clear even at a technical language level. As a consequence, they will be drafted by trying to balance the legal and the technical aspect of the present several definitions. There are essentially two research questions in the thesis. The first one is "What is the future of the regulation of the IoT? Will the proposed AI Act be a model for IoT regulation? If yes, in which way? If not, which other EU legal acts might be employed, and will they need to be updated?" The main idea is that the AI regulation might also be applied to IoT applications that are considered high risk, whereas for domestic IoTs, which are generally considered to be low-risk applications, EU consumer and contractual law will still apply, hence the importance of the PLD.

Chapter II deals with the first part of the state of the art and the history, structure and future evolution of IoT technology into IoE technology, within the home environment. The first part of this section is dedicated to the history of the IoT and to the relationship with the theories of ubiquitous computing and ubiquitous sensing. The main objective is to show that the IoT is a concept that evolved through time, based on predictions and prototypes made in the '90s. The result of these theories and predictions is this general and easily applicable technology, the Internet of Things, that can be adapted to several sectors such as agriculture, industrial automation; healthcare and the home. In order to understand better, there is a description of the function and composition of the main parts of the IoT, meaning sensors, gateways, the cloud, the fog and the actuators.

In the second section of the chapter, the focus is on the concept of the smart home. Its origin dates back to the 1930s (when it was considered a paradigm of luxury). This idea then evolved through the '70s and '80s into the first prototypes of connected homes. The first examples had either a utopic character, such as in the US with the Xanadu homes, or their target was just research as in Japan's prototypes, possibly with the idea to apply its results for the needs of a rapidly ageing population.

However, the idea of the smart home and of the IoT could not be understood if not in connection with the theory of ubiquitous computing. The smart home was merely an application of ubiquitous computing as it should have been a fully connected environment, as it still is in the minds of IoT objects creators-designers. Today, the smart home is just a partly connected environment: some parts of it might be able to interact with us, but there are often interoperability problems with other smart appliances. Nevertheless, despite the prospective future advantages of the smart home in terms of environmental sustainability, intergenerational solidarity and general fairness for human relationships (e.g., to help both ageing and disabled people), the smart home has not been a success so far, due to policy-sociological and technical reasons. As far as policy is concerned, the "smart-home" idea developed first in connection with the field of smart-grids and energy policy more than the IoT and EU private law, hence it was perceived to be "technical-niche". With regard to the sociological reasons, research studies also showed that elderly people did not have sufficient digital literacy to become truly proficient in "governing" a smart home. However, this might change in the near future, given that most ageing adults are now digitally literate, even if at only a basic level. One other reason that slowed down the creation of the smart home was that, even for consumers, privacy mattered and came across as a powerful reason not to buy cheap home gadgets. Apart from the above-mentioned sociological reasons, there are also technical factors that have been slowing down the appearance of the smart home. These factors are essentially two: the slow pace in adopting 5G technology and the lack of interoperability standards. On the issue of standards, the new proposal of the Data Act is likely to be the legal basis for the Commission to approve harmonised standards in addition to the perspective cyber-resilience act proposal[5]. However, even in that case, problems of liability and accountability might subsist. There will be some examples making reference to the lack of liability rules concerning technological standards.

In the second part of the chapter, there are several alternatives for categorising smart objects in the home, by accepting the fact that whoever studies these issues has to deal with a situation of an "incomplete" smart home. The first criterion accounted for was the one based on the novelty of the object: in fact, the majority of the smart objects we have in our home are mostly a more "evolved" stage of a previous one (e.g., a smart thermostat or dishwasher) but there also are completely new objects such as integrated voice assistants, such as Amazon's Alexa and its tangible container, Echo dot. Another criterion could

[5] More on cybersecurity issues and the IoT can be found in Chapter III, 4.

be based on the level of autonomy of the object itself and another one is based on their main function. Further, there could be one last criterion which is based on the function of the object. It is definitely the most important for the consequences in terms of EU law, but it is likely the trickiest one to apply. In particular, IoT objects that are defined “wearables” often mix consumer-commercial functions, such as telling the time, with healthcare functions (such as emergency data transmission in case of irregular heartbeat to public emergency numbers) and it is becoming increasingly difficult to tell apart which function is which and which is preponderant. Finally, in a third section, there is a list of the technological changes occurring within the IoT due to sustainability issues, concerns about the structure of the internet and data privacy issues. That is why I also expanded on the newest technologies that are starting to make the current IoT structure “hybrid”, i.e., Edge Computing, Blockchain, DLT and, finally, new research into bio, not rare-earth-element-reliant and non-toxic material for the IoT, the Green IoT.

Chapter III is written by combining two criteria: a chronological one and a thematic one. I systematically reviewed all the EU law that is already applicable to the home IoT objects, or that is still discussed during the legislative procedure, to find out that there is no comprehensive discipline on IoT objects. Relevant rules are scattered across different thematic blocks. The first block of legislative acts concerns what in this thesis are called “data laws”: EU legislative acts or proposed acts which are impacting or most likely will impact the IoT by focusing on the data processing aspect of this technology, such as the GDPR, the e-privacy directive, the Free Flow of Data regulation and the proposed Data Act. For each of these documents there is a highlight on the points of friction with IoT technology. In particular, the aspect of IoT technology that is most in contrast with the protection of fundamental rights is the indiscriminate data collection of both personal and non-personal data in the home, in connection with “shaky” legal bases for data processing, especially as far as consent as a legal justification for processing is concerned. It will also be discussed whether the proposed Data Act can actually empower consumers by giving them the chance to access and avail of the data produced by an IoT object. Secondly, there is a review of the whole EU private law acquis which is divided into two parts: first, a list of the documents that were created when the IoT started being commercialised. I then attempted to explain the structures and the consequences for liability of directives EU/770 and 771/2019, on the sale of goods which considers as goods also objects with interconnected digital elements (SDG) and the supply of digital content or digital services (DCDS). Further, I analysed how the EU Commission is trying to update some parts of the consumer *acquis* such as the Unfair Commercial Practices Directive (UCPD) and the Unfair Terms Directive (UTD) by trying to connect them to the GDPR, to the previously cited SDG and DCDS directives, buts also trying to harmonise them with the New Consumer Agenda and the New Green Deal. Finally, there is a brief description of how the European Electronics Communications Code (EECC) and the NIS I and NIS II Directive, which concern more cybersecurity and telecommunication regulations, are going to influence the SDG and the DCDS for the growing interoperability and security obligations that these objects will have.

The last part of the chapter is dedicated to the policy efforts concerning the regulation of the AI and why the IoT seems to have disappeared for a long time from the EU Commission legislative process. I argue that IoT applications which will be considered “high risk” (e.g., surgical robots, autonomous cars) will be assimilated to the regime of high-risk AI algorithms based on an interpretation of the proposed AI act. On the contrary, low-risk applications, such as domestic IoT objects, will be subjected, in theory, to the wide array of the EU legislative acts and proposals cited. Given that smart home objects are consumer objects in their very essence, their liability issues will be connected to product liability issues in one way or another. Moreover, in this chapter there is a short introduction about the extreme relevance of the product liability directive and its ongoing reformation process, and I argue that the main EU legislative act regulating liability will be the future EU reformed PLD, which will need to interact with the GDPR, the Data Act and the two directives SDG and DCDS.

Chapter IV focuses on the state of harmonization of liability in the EU and on the different liability regimes and their importance to society. In a first section of this chapter, the main kinds of liability (tort, strict, pre-contractual and contractual liability) are reviewed in light of their level of EU harmonization. In general, what was mostly harmonised were remedies and duties of the parties but not the founding definitions of liability such as for the validity of the contract or the concept of fault. This section proved that the most structured and still not formally updated system of harmonised liability is the PLD. In the second section of this chapter, liability is studied by adapting not only a legal point of view but also a historical and sociological one. Building from that, the research shows that liability is not just a legal remedy but also is a powerful tool to help businesses invest in innovation and people to eventually trust technology. In the last part of the first section I delve into the liability applied to the smart home. I argue that the COVID-19 pandemic has radically changed consumers’ expectations about the environment they live in, which is already leading to a re-definition of the spaces we work and spend time in. This will most likely impact consumers’ perception of the home and the technology in it, and it will contribute to characterising and defining our idea of liability for domestic objects.

The second part of this chapter instead is more focused on an EU institutional approach to private liability for smart domestic objects. Especially now that there is the intention to update the PLD, it is important to understand whether the legal basis that has been used so far (in practice just Article 114 TFEU) is really the most adapted legal basis to adopt acts concerning the Digital Single Market. That is why there is a part in this subsection which discusses how the principles of conferral of competences, subsidiarity and proportionality could be applied when liability of digital technologies, such as the IoT, is involved. As a matter of facts, the Commission in all its accompanying memoranda to the proposal for the Digital Single Market did not care to clarify the connection between the Single Market, whose aim is regulatory and focuses on the maintaining of the four market freedoms, and the Digital Single Market. The first

reply might be that the Digital Single Market is actually a part of the Single Market. However, given the importance that fundamental rights have always had in digital single market history, starting with the GDPR data protection objectives and continuing with the recent declaration of the Charter of Digital rights, one could wonder whether Article 114 TFEU should be reformed and include the digital single market too, especially as a legal basis for a new PLD.

Chapter V's focus is on the PLD. This is motivated by the fact that already in chapter III, it was ascertained that the updated PLD will be the EU legislative act that will be covering liability issues of domestic IoTs. The chapter is divided in three main subsections. The first one addresses the legal history and legal comparative models. In this part, as a form of introduction, the PLD main articles are described summarily, in order to better understand the further analyses of the PLD. Several national models of product liability theories are outlined, and one hypothesis is formulated: that the systems that were traditionally more protective of consumers (such as the French, the Danish, the Spanish and, for some aspects, the pre-Brexit English ones) would be the ones which would have their rules challenged the most through the preliminary reference to the CJEU or through infringement proceedings initiated by the EU Commission. Moreover, there will be a synthesis of the debate concerning the true function of the PLD, which the majority of scholars now believes is just to protect the internal market and does not have a consumer protection function.

The second subsection of this chapter is divided into two subparts and might be one of the most distinctive features of this thesis. Each subpart consists of one case study relying on the case law involving the PLD before the CJEU. It is considered important to use a more scientific approach in order to understand what the PLD shortcomings were and why they happened and how they are going to affect the update of the PLD for new technologies. These case studies both employ a quantitative and qualitative method of analysis. That is why I selected the judgments from the EURLEX database, schematised the text of both the judgments and the opinions of the Advocates General (AG) into a table, to understand whether the final published document differed from the AG's opinion and to identify how many times the articles of the PLD were involved before the CJEU. Firstly, I found out that the countries who had the most protective legal models pre-PLD were also the ones which were challenged most before the CJEU, thus confirming the hypothesis of the previous subsection. Moreover, I discovered that Article 3 PLD concerning the notion of producer and Article 13 PLD concerning the PLD relationship with national liability theories were the most challenged. Especially Article 13 PLD is worthy of further discussion. From the analysis of all the corpus of cases, it emerged that there were two periods in time, chronologically distinct, in which Article 13 was important. The first period was characterised by a series of judgments such as *Commission v. France I*, *Commission v. Greece*, *Gonzalez Sánchez* and *Skov Æg*[6], in which, through the interpretation of Article 13 PLD, the PLD was considered a maximum

[6] References to these judgments can be found in Chapter V section 2.

harmonization directive. This meant that national no-fault based systems of liability similar or more protective than the PLD could not be applied. Instead, other liability schemes involving contractual or tort liability could survive alongside the PLD only if they were special and they existed before the notification of the directive. In the second chronological period (from 2004 until now), Article 13 PLD was indirectly challenged: in this phase, the courts were asking the CJEU through the preliminary reference whether national substantive and procedural laws could be considered compliant with the spirit of the directive such as in *Novo Nordisk Pharma* and *Sanofi Pasteur*[7]. In summary, Article 13 PLD is the most important article of the PLD as it touches upon the difficult application of the distribution of competences principles between the MS and the EU, as already explained in Chapter IV. That is why, ultimately, the text of Article 114 TFEU should be changed to implicitly include the digital single market, so that fundamental rights could also be protected better.

The third section could also be considered as the second most distinctive feature of the thesis. In the third section there is a comment on the articles of the PLD that were mostly challenged and that were susceptible to be changed because of the impact of the IoT. Each of these articles will be commented by relying on three methodological steps. Firstly, the selection of the article to be amended relies primarily on the results of the quantitative studies. Secondly, the twin directives SDG and DCDS will be used together with the GDPR in order to select the articles that could be challenged by new technologies and that might not have been highlighted by the results of the previous case studies. These legislative EU acts also contain regulatory and legal models that could inspire the update of the PLD. Thirdly, in order to make the analysis more complete and to include a legal scholarship perspective, the documents released by the European Law Institute (ELI) on the update of the PLD will also be employed together with the opinions of the representatives of European insurances groups. This will allow an assessment of the different solutions proposed and, possibly, new ones to be suggested which will be summarised better in the conclusion parts, as they will also benefit from the insights of the last chapter of the thesis.

As anticipated, Chapter VI is the part of the thesis which is mostly built on a comparative law approach. As the PLD was partly inspired by the US Restatement of Torts, Second, and because the IoT was first created in the US, the American model of products liability seemed an interesting point of reference for the future update of the PLD. Also, compared to the EU, in the US there were many more cases involving the products liability of domestic IoT objects. The objective of this last chapter was thus to analyse the history of the many and varied theories and remedies which address the problem of ordinary objects injuring their users and how these theories might develop through the use of IoT technology in a domestic environment.

This chapter is divided into two parts, the first of which is dedicated to the evolution of the several products liability theories which created the almost unitary concept of US products liability. In order to do so it was important, on the one

[7] References to these judgments could be find in Chapter V, section 2.

hand, to remember the specificities of the several kinds of liability in the US (contractual, tort and strict liability). And, on the other hand, it was important to keep in mind the vast array of legal formants of rules and remedies concerning the products liability theory such as national court judgments, Supreme Court judgments, federal statutes, national laws and authoritative scholarly documents such as the Restatement of Torts, Second and Third. The analysis of US products liability history (which is mainly written for European legal scholars) also reflects the characteristic allocation of checks and balances of the US from a constitutional point of view. Unlike in the EU context where there actually is a PLD that is implemented in all MS and which coexists with national liability rules that are applied when the PLD cannot be, in the US there is no such federal unitary legislation on consumer products. This, however, does not mean that all these theories are not perceived, in their difference, as a unitary part of law because of their application field.

In the second part of this first section there is an attempt at summarising the trends and evolutions of the US technology regulation approach, which was not usually characterised by huge state intervention. Through the research of recent policy documents some trends were individuated. Apart from platforms, for which big changes in regulation through competition law are expected, there is only The Internet of Things Cybersecurity Improvement Act of 2020 concerning cybersecurity for the IoT at the federal level, which defers the competence to standardise and establish good cybersecurity practices concerning the IoT to the NIST[8]. There are no statutes at a national level concerning the IoT and products liability. However, California does have new cybersecurity and data privacy rules concerning connected objects (IoTs) but the statute that introduced them has several shortcomings including the impossibility for private parties to rely on it for legal actions. The third part of this first section addresses American legal scholarship and tries to explain why US scholars almost never make reference to IoT technology in their scholarly works.

The second section of chapter VI deals with the growing corpus of cases that concerns domestic IoT objects. The first group concerns objects used for the security and surveillance of the home: IP-cameras, routers, smart-locks but also smart televisions used for surveillance purpose by their producers. Most of the proceedings in this sub-sub-section are carried out by the Federal Trade Commission (FTC). The FTC can initiate proceedings whenever data security and data privacy are involved, and when, according to the lexicon of Section 5 of the FTC Act, there has been a misrepresentation of how the product should work or whether there was an unfair practice of the manufacturer on consumers. Constitutionally, data privacy and security are parts of consumer protection policy.

The other judicial cases concerned smart-locks, smart toys, and connected cars. These cases are indeed products liability cases as plaintiffs tried to use some of the theories mentioned before in the “historical” subsection (in particular implied and express merchantability warranties but also negligence),

[8] National Institute of Standards and Technology.

even if the products liability aspect is rarely explicitly mentioned. However, in these cases there are several claims concerning the harm from personal data breach which often coexist with “more traditional” products liability claims. Often, however, judges refused all these claims by applying a very strict interpretation of the Supreme Court cases *Clapper* and *Spokeo*[9] on legal standing. Especially as far as the proof of data harm is concerned, it is very difficult for plaintiffs to prove how a personal data breach affected them. The cases concerning IoT with medical functions have clearer product liability claims (negligence, failure to warn and strict liability claims mostly) but they also face another kind of filter which is the pre-emption clause of Section 360 k of the Medical Devices Amendments Act of 1976 (MDA). This clause allows the producers of high-risk medical devices to be exempt from liability unless the plaintiffs show that there is an express violation of federal requirements. The Supreme Court with *Riegel* interpreted this clause very strictly, hence for plaintiffs there is basically no remedy unless the courts allow them to use the FDA’s good manufacturing practices as federal law that was infringed. It will be a problem for the years to come for legal scholars and judges to find ways to establish attainable proofs of the level of data harm in order to overcome the legal precedents but, at the same time, these attainable levels of proof of data harm must not be so low that courts could be snowed under with petty complaints. That is likely to be the same problems in the EU, when product liability and data protection damages will start to arrive in the national courts and the CJEU. There will be a problem to find a reasonable way in order to filter petty complaints from more serious ones.

To sum up, the analysis of the US product liability theories combined with the observation of the US approach to regulate IoT technology was an insightful process. It proved to be a filter through which I could analyse cases that involved products liability issues in a more complete way. In the US, product liability claims will arise together with data privacy issues. All the theories concerning data harm might in time become part of the remedies forming the varied product liability category. After all, data privacy is part of consumer protection at a constitutional level, as well as products liability. This process might have already started given the use of the FTC consumer protection instruments of Section 5 of the FTC Act in order to deal with data privacy and data security issues.

Finally, the conclusions chapter outlines the research results obtained through the application of the multi-faceted methodology of chapter I in orderly, involving both a technological focus and more traditional legal methods, such as legal comparisons. The results are of three main types:

- The first kind of results could be defined as systematic/organisational results. Some examples are a new organisation of the technological state of the art and of the meaning of the word smart home. Also the list of all the EU private law acts that could be applied to the IoT is to be placed in this category.

[9] References in Chapter VI.

- The second kind of results are analytical results. They allow reflection on the previous set of results and discovery of past and future trends. Specifically, the two case studies on the CJEU PLD-related case law belong to this kind of results.
- The third type of results are creative results. They go further than the analytical results and try to imagine practical or policy implications by the previous analytical results. One example of this kind of result is the list of articles of the PLD that will most likely be interested by the PLD update.

In conclusion, this thesis claims that the evaluation of the state of the art, both legal and technological, combined with a holistic understanding of the notion of liability leads to the conclusion that the intersection of these elements is the PLD. The PLD is the most relevant act of the *Consumer Acquis* that has not yet been updated. In order to understand whether there was a true need for its rules to be updated, the PLD was analysed and commented in light of previous case law and through the most relevant EU legal acts (such as the GDPR, the SDG and the DCDS) which can offer models and ideas about how technology can influence a legal text. It was demonstrated that the technological characteristics of the IoT require a change in the PLD and in the TFEU and some practical examples and suggestions will be given at the end of Chapter V. However, the analysis could not have been complete without a comparison with a different legal system. Choosing the US system of products liability as the model of comparison will give valuable insight, especially considering the higher number of product liability cases involving IoT domestic objects compared to the EU. This can compensate for the lack of cases involving IoT objects before the CJEU and can give a more practical idea of what product liability cases would entail. Finally, it will be claimed that, whatever the update of the PLD may be, it will be important not to leave consumers without substantial access to legal remedies as happened in the US for several cases, especially the ones involving medical IoTs. Especially when the damage is serious, it will be important that the procedural rules of the MS which implement the PLD are also structured in order to respect the principles of equivalence and effectiveness under EU law.

Chapter I – Methodology

Chapter I – Methodology 12
1. Introduction 12
2. The main features of the research 12
3. The question(s) addressed in the research 14
4. Exclusions from the research field 15
5. Provisional Answer, social significance of the research and objectives 16
6. Definitions 17

1. Introduction

This chapter serves several purposes, namely (1) to explain the features of this research (2) to explain the questions posed in the research (3) and to understand both the limitations and exclusion of this research (4). It will also be a space dedicated to providing provisional answers and to briefly illustrate the social significance of the research (5), while also providing some entry-level definitions of the words that will be used most throughout the thesis (6).

2. The main features of the research

The characteristics of this research are initially identified by its title. This thesis mostly focuses on the legal aspects of the Internet of Everything [10] and the Internet of Things [11] in the home environment. Therefore, the majority of this thesis will actually be a traditional legal thesis, based on the analysis of legal documents, such as laws, legal act proposals and case law. Nevertheless, these sources will be selected through the filter of EU law. Regulations, directives and decisions, EU judgments and also policy documents and proposals will be analysed by focusing on the topic of liability, which will make this thesis more monographic in character, as it will address product liability in particular in its two most innovative chapters, i.e., chapters V and VI. This is due to the fact that the aim of this work is to create a set of insights and guidelines concerning liability for the connected home. As connected home objects are able to transfer data among EU Member States (MS) and beyond, it is advisable to try to find a common approach that the MS could adapt to their own needs.

In order to understand the many facets and the interdisciplinary character of this research, there will also be a general overview of the documents and legal

[10] Internet of Everything. The definition of IoE is at (6) of this chapter.
[11] Internet of Things. The definition and explanation about why the term IoT is used more than IoE is in subsection (6) of this chapter.

acts that might be relevant to the smart home, the IoE, the IoT and to liability matters. The intent is to show that each legal field explored is connected to the others. The aim is also to provide readers, even those not well-versed in law, with a filter to understand how connectedness is not only an effect of technology but also a characteristic of the law that is applied to technology. This will mainly occur in the chapters devoted to the state of the art, such as Chapters II and III. In particular, Chapter III is a brief summary of the most important legal and policy documents that are, as of now, applicable to the IoE in the home, while Chapter IV, introduces the theme of liability as a criterion to include other elements in the analysis, such as the notions of the smart home's social accountability and environmental liability.

One important element to state at this point concerns case law. The Court of Justice of the EU (CJEU) has not yet rendered a judgment on a domestic connected object, such as a small robot or a voice assistant. Hence, the cases selected will be either dealing with IoT technology aspects relevant to the thesis (e.g., judgments on software or on data processing), or with regulation models that could be adopted in order to draft a EU legal act proposal concerning such IoE objects (e.g., cases related to medical devices and product liability). The EU case law will be mostly concentrated in Chapter V and will mainly concern the application of the Product Liability Directive (PLD)[12]. Where possible and whenever relevant to do so, the EU case law will be compared with the different legal rules and remedies of the Member State (MS) in which the case originated before being analysed by the CJEU. Moreover, in Chapter VI this comparison will be more explicit as the entire chapter revolves around the US products liability system. The US was considered to be a good choice as a term of comparison. In fact, the IoT technology underpinning the IoE and the concept of smart home was actually first created in the US. Moreover, in the US there are many more products liability cases concerning IoT domestic objects than in the EU. This reference will prove successful in providing insights not only into how to update the current product liability system in the EU, in order to make it more adapted to new technologies such as the IoT and future IoE, but also to make accurate forecasts concerning changes in national procedural laws. These legal changes must be enacted in order to avoid people not having effective remedies against new technologies, but also to prevent national and European courts being overwhelmed by petty complaints.

With regard to EU law, it is also important to take into account that this is still a period of transition for the regulation of new technologies. There are countless

[12] "Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products *OJ L 210, 7.8.1985*, p. 29–33," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A31985L0374 . Hereinafter, PLD.

policy initiatives, from the Green Deal[13], to the European Digital Strategy[14] and the Recovery fund[15] which could potentially benefit future domestic connected IoE devices. Nevertheless, at the moment of writing, there is not yet a comprehensive legislative document concerning liability of these technologies, which could have been a useful base from which to start the research. Despite that, between 2020 and 2021, there were several interesting legislative proposals concerning not the domestic IoE directly, but distinct aspects of the regulation of AI and data[16], which are issues that will be discussed limited to their relevance to the thesis. The list of the most relevant proposals and current EU legislative act that could be applied to the future domestic IoE will be explained in the State of the Art section and particularly in Chapter III.

This however is not only a legal thesis. I believe that it is not possible to figure out liability solutions for the smart home without first understanding its complexity (whose underpinning technological paradigm is the IoT, see *infra* 1.5). In chapter II, there will be a brief, but complete and precise account of how this technology works and what the main IoT applications in the home environment are. Preliminary information must be provided in this context: the person writing this thesis is not a technical expert, but they will try to provide the best explanation of how the IoT and a smart home works, also for lawyers. In this way, the research will acquire a multidisciplinary character. In Chapter II, I will try to explain how the IoT paradigm was born, the goals for which it was created and what it meant for the creation of the smart home paradigm.

3. The question(s) addressed in the research

The issue to be investigated is the adequacy of current EU private law system in relation to the challenges that the IoE and IoT systems for the house will bring forth. The research question can be detailed as such.

- Is the current IoT environment for the home in need of new rules to allocate civil liability?

---

[13] "COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS The European Green Deal, COM/2019/640 final," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2019%3A640%3AFIN, hereinafter Green Deal.

[14] "COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Shaping Europe's digital future, COM/2020/67 final," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0067&qid=1661352744218.

[15] "Regulation (EU) 2021/241 of the European Parliament and of the Council of 12 February 2021 establishing the Recovery and Resilience Facility *OJ L 57,* 18.2.2021, p. 17–75," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0241&qid=1661352828053.

[16] "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTSCOM/2021/206 final, "EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206&qid=1661352946581 . Hereinafter AI Act or AIA.

- It is suggested that new rules are required but it will be investigated whether these new rules
  - are rules that already exist and which can be adapted to these new scenarios; or
  - if existing rules cannot be adapted beyond a certain threshold, it will be investigated how the current private liability rules can be changed into new ones. Furthermore, if new rules are required, it will also be investigated whether there will also be the need to adapt them to the future and more encompassing IoE.

4. Exclusions from the research field

The problem with liability is its vast meaning and applicability through an extremely diverse range of legal (and other) subjects (see Chapter IV). However, for reasons of time and also constraints regarding the theme of the thesis which, in the "expected results" section of the grant explicitly mentions the consequences for consumers[17], the application of the expression "legal liability" is limited to the sphere of EU private law. With EU private law we intend the *acquis*, meaning all EU law concerning both consumers and contracts. I used the term "limited" as an understatement, as EU consumer law field is quite vast. The choice of narrowing down the field of analysis was also dictated by time constraints and also by an ever-evolving state of the art (both from a technological and from a legal point of view). Despite keeping the state of the art updated constantly throughout the duration of the PhD, the final policy/ legislative documents and judgments considered do not go beyond 31 August 2022.

As far as the extent of the meaning of private law liability is concerned, Chapter III will have the function of a filter. Given that the reply to the first issue concerning the need for new rules will be a positive one, as the characteristics of present IoT technology are at odds with both consumer and data protection models in the EU, it was also decided to assess all the consumer and contractual *aquis* in order to find which kind of EU legislative act, if such exists, could be applied to the liability of IoT objects for the home.

Until now, despite the proposal for an update and the legal debate, the PLD is the only document concerning liability that is directly applicable to IoT objects which are low risk, as the ones we have in our home are generally considered. PLD liability will always be compared closely to the liability arising from the breach of data protection rules. According to the different legal traditions, liability arising from data breach is simply a non-compliance liability[18] and therefore more akin to administrative liability. However, I will consider Article 82

[17] Part B, p.24, Grant Agreement, LAST-JD-RIoE EJD, N. 814177.
[18] Christiane Wenderhorst, "Strict Liability for AI and other Emerging Technologies," *Journal of European Tort Law* 11,2 (2020):157-158, https://dx.doi.org/10.1515/jetl-2020-0140.

GDPR concerning liability in depth as a gateway which is able to connect compliance issues with private law ones.

Furthermore, I will not address possible criminal liability issues of IoT objects in the smart home, not because the theme in itself is not interesting, as indeed it could indeed inspire both a legal and a philosophical analysis. However, there are already a considerable number legislative acts on EU private law that will be used for this thesis, as EU private law encompasses both contractual and tort liability (this latter category also includes strict and product liability). It is wise not to risk addressing a theme such as the criminal liability of new technologies in haste.

With regard to the domestic objects to be analysed, there is a methodological problem. As will be explained in Chapter II, there are new connected objects for the home which are marketed every day. It is impossible to analyse them all and I will try to provide some criteria to categorise them. After explaining how these objects can be categorised, I will focus on the ones that: a) are more complex technologically and require the use of modern AI such as voice assistants and b) that combine different functions, especially healthcare and consumer functions within the home environment.

5. Provisional answer, social significance of the research and objectives

Especially in Chapter IV, I will demonstrate that the reasons for which liability rules have been created over the centuries do not change. What changes is the ability of a liability system to adapt to new challenges. Specifically, ascertaining causality in liability cases involving connected home objects can be complicated at times by the large number of stakeholders involved and new ways for these objects to function. There is no longer only one producer of a present-day IoT object, but operators (e.g., software producers, cloud services providers and platforms) could be different entities from the manufacturer and, despite that, bear, *de facto*, a significant degree of responsibility in creating products that may turn out to be defective or unsafe. It is advisable to take a technologically focused perspective to understand how the IoT environment functions, also relying on the categories of data protection and analysing “new” sources damages, if any. As a matter of fact, the most interesting findings will concern whether new immaterial damages arise from the functioning of domestic IoT objects and the main assumption is that the current way of processing data (both personal and non-personal) will be the main source of known and unknown damages. Moreover, data protection and liability claims will have the tendency to be made at the same time, especially when the IoT is used in a domestic setting. This may happen in the EU as the data subject in this case is almost always a consumer. This assumption will also be reinforced by the fact that in the US, a similar phenomenon is already happening in a series of cases involving different home IoT objects: from the ones having surveillance functions to the ones that also perform medical functions and that are used in the home environment.

As far as the social significance of this research is concerned, it is vital both for consumers and for businesses to understand what kind of rules apply in a new context such as the connected house in the aftermath of the pandemic. IoT devices for the home and especially the ones that can always stay on our person (wearables) could make life easier for certain categories of people, such as not-fully autonomous elderly people and people with disabilities. In addition, domestic IoT objects could also help consumers in having their health monitored, especially during a period of rehabilitation and so as to avoid overcrowded hospitals. Moreover, smart metering could make a home's inhabitants more aware of their energy consumption and be more effective in changing the sustainability of their habits for the sake of the environment's sake[19].

There are primarily two objectives. The first one is to give a systematic order to the EU private law legal corpus about the IoT in the home by focusing on the theme of liability, which is an aspect that is seldom directly developed at the EU level, as it does not have an exclusive competence to regulate it[20]. The second objective is to contribute to the debate about the update of the PLD.

6. Definitions

Some operational definitions of the most common words used throughout the thesis are provided here. Most of the definitions are legal-technological definitions given by the EU. They will be put into context throughout the thesis and may be subjected to a critical analysis. Their function here is to give the reader an "entry level" understanding of their meaning through which the discussion will then be developed.

AI system: I will adopt the proposed notion of the AI present in the draft of the proposed AI regulation. AI is not a single technology but a system of different ones. According to Article 3 of the EU proposed regulation of AI an "artificial intelligence system" (AI system) means "[…] *software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with* […]"[21]. Annex I includes the following techniques. "[…] *(a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;*

(b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;

[19] More details on this in Chapters II and IV.
[20] See Chapter IV.
[21] "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS
COM/2021/206 final," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206 .

(c)Statistical approaches, Bayesian estimation, search and optimisation methods". This definition is important as it represents the first attempt to define what an AI system is from a regulatory point of view, in the EU. However, there are not as many applications of AI for domestic connected objects as one may think. The majority of AI applications in connected domestic objects (for which the definition of AI system is relevant) are not located in the device but are applied in the cloud (especially Machine Learning, ML algorithms). However, the legal modelling of AI will also be influencing the liability of other technologies, IoT included, especially if these devices use algorithms that are considered as high risk. This will be explained further in Chapter III.

Consumer: the selected definition for consumer is the one from the Consumer Rights Directive (CRD), as it is quite clear and a good point from where to start an analysis. In the context of the CRD, the "[…] *consumer means a natural person who acts outside the scope of the business, trade or craft*"[22].

Data: at this stage, only an operational definition of data is considered. Data is the vehicle of information, in technical and legal terms, which can be seen both as a commodity and as enabler of fundamental rights.

Data Protection: a field of law that is separate from the right to Privacy[23] and that mostly concern the issues connected to unfair and unlawful personal data processing. In the EU it is also a fundamental right enshrined the Charter of Fundamental Rights of the EU (Art.8) and Article 16 of the TFEU.

Domestic: of the home.

Personal data: For the purpose of clarity, we will use the definition set out in Article 4(1) of the General Data Protection Regulation (GDPR)[24] as "[…] *any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical physiological, genetic, mental, economic, cultural or social identity of that natural person.*"

Non-personal Data: What is not covered by Article 4(1) of the GDPR. To make it more effective, data that can be processed in house and that do not reveal *prima facie* an identified or identifiable person.

IoT: Internet of Things, IoT, previously known as M2M (Machine to machine communication) technology[25]. It indicates the technology that connects

---

[22] "Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council Text with EEA relevance *OJ L 304, 22.11.2011*, p. 64–88," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32011L0083&qid=1661353206931 .

[23] In the US, Data Privacy is used more than Data Protection and it finds its grounds not in an autonomous data protection right, as in the EU legal order, but generally in consumer protection regulation. Shawn Marie Boyne, "Data Protection in the United States," *American Journal of Comparative Law* 66,8 (2018) 28, https://dx.doi.org//10.1093/ajcl/avy016 .

[24] "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) *OJ L 119, 4.5.2016,* p. 1–88," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679&qid=1661353452590.

[25] Kevin Ashton, "That 'Internet of Things' Thing". *RIFID Journal*, 2010.

things with humans and things with things. Its dual nature comprising the Internet (the digital) and things (physical reality) has made it difficult to define[26]. In a descriptive way, the Internet of Things is an infrastructure of sensors, actuators and electromagnetic waves that can collect and process data from an environment and is able to give an intelligent reply[27]. It is the technology that is mentioned the most throughout this thesis as most of the relevant literature refers to it.

IoE: The Internet of Everything is the next step on from the Internet of Things as "[…] *it encompasses not only devices but also individuals and data*[28]. This is more of a systematic definition and not a technological one. As will be explained in Chapter II, the IoE and the smart home, are not yet a reality. In addition, all the literature on smart domestic objects keep referring to the IoT. That is why I will use the term IoT more throughout the thesis. However, this last term will need to be interpreted with a feature of future all-connectedness, which will tie it to the initial definition of the IoE.

Liability: it is the legal remedy which allows a party, under certain circumstances, to receive compensation in money or other form, because a previous (contractual) or sudden (extra-contractual) relationship has been breached. Liability can have multiple functions. The first one is an enabling function, as it offers rules according to which one can exercise rights in society. The second one is a compensatory function and offers the means to repair the damage done and re-create (through money or other reparatory activity) the factual situation before the damage. The third function is the punitive/dissuasive one, in order to ensure that the one who caused the damage is convinced to no longer cause damage to anyone else. In this work, it will also encompass soft law concepts, such as accountability, and also will cover the endeavours of environmental sustainability. More on the social and legal functions of liability can be found in Chapter IV.

Processing: According to Art. 4(2) of the GDPR, processing means "*any operation or a set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*;".

Producer: According to Article 3 of the Product Liability Directive (PLD), the producer *"*[…] *means the manufacturer of a finished product, the producer of any raw material or the manufacturer of a component part and any person who,*

---

[26] Debasis Bandyopadhyay and Jaydip Sen, "Internet of Things: Applications and Challenges in Technology and Standardization," *Wireless Personal Communications* 58,1 (2011): 49-69. http://dx.doi.org10.1007/s11277-011-0288-5.

[27] This definition is an elaboration from Bandhiophaday and Sen's (*op.cit*), Perry- Roda's, and Pagallo, Durante, Monteleone's (2017) works. See Susan Perry and Claudia Roda, "The Internet of Things," in *Human Rights and Digital Technology*. *Digital Tightrope*, Susan. Perry and Claudia Roda (London: Palgrave Mc Millan,2017), 132 https://link.springer.com/book/10.1057/978-1-137-58805-0; Ugo Pagallo, Massimo Durante, Shara Monteleone , "What is New with the Internet of Things in Privacy and Data Protection? Four Legal Challenges on Sharing and control IoT," in Ronald Leenes, Rosamunde van Brakel Serge Gutwirth and Paul De Hert, *Data Protection and Privacy: (In) visibilities and infrastructures* (Cham: Springer 2017),59-78 https://link.springer.com/book/10.1007/978-3-319-50796-5#about . More on the history of this technology see Chapter II.

[28] "IoE", Last JD RIoE Website. 2019, Accessed on 31 January 2023, https://last-jd-rioe.eu/ .

by putting his name, trade mark or other distinguishing feature on the product presents himself as its producer[…]"[29], which includes also the importer (Article 3.2 PLD) and also the supplier whenever neither the producer cannot be identified (Article 3.3 PLD).

Smart: the adjective smart, in all the expressions that will be used in this thesis means that something, such as an IoT object, is connected to others in an intelligent/reactive environment. The connection means that the said environment and the various parts that compose it are able to interact with each other and the user/data subject in a meaningful way through the collection and analysis of human inputs which ultimately become data.

Smart appliance: part of the house that allows the passing of energy and meaningful contacts with other devices[30] and humans.

Smart house/smart home/home IoT: the environment of the home that is enhanced through IoT and its interaction with the inhabitant(s) and each of its parts.

Trader: The concept of trader of the Consumer Rights Directive is adopted, which is set out in Article 2(1). Trader' means any "[…] *natural person or any legal person, irrespective of whether privately or publicly owned, who is acting, including through any other person acting in his name or on his behalf, for purposes relating to his trade, business, craft or profession*"[31]. The choice of this definition depends on the fact that it was the first one to describe this legal subject and it influenced all the other definitions of it that are used by other EU legislative acts.

[29] "Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products *OJ L 210, 7.8.1985*, p. 29–33-" EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31985L0374 . Hereinafter PLD.

[30] Tiago Serrenho, P. Bertoldi, *Smart home and appliances: State of the art. Energy, Communications, Protocols and Standards*. (Luxembourg: JRC, 2019).

[31] Article 2(1) CRD.

Chapter II - State of the Art part I: the IoT technology and the smart home

Chapter II - State of the Art part I: the IoT technology and the smart home 21
1. The state of the Art 21
2. The IoT history and struggles for a definition 22
3. The IoT structure 25
3.1. The technological side: sensors 26
3.2. The technological side: actuators 29
3.3. The technological side: the gateway 30
3.4. The technological side: the cloud 30
4. The smart home and the IoT paradigm 31
4.1. Is the smart home yet to come? 32
4.2. Why the smart home is not here to stay yet? 36
5. Functional taxonomies for the IoT in the house 41
5.1. The novelty criterion 41
5.2. The autonomy criterion 42
5.3. The EU Commission classification of Consumer IoT 43
5.4. Mixed functions home IoT objects 44
6. Future technological perspectives 45
6.1. Fog and Edge computing 45
6.2. Distributed Ledger Technologies and Blockchain for the home 47
6.3. The new Green IoT (GIoT) 48

1. The state of the art

As already specified in the methodology section (Chapter I), it is essential to know how IoT technology works in order to understand how it will impact present and future liability rules. The first part of this chapter consists of three main sub-sections. The first one of these subsections has an introduction character (1). The second sub-section will summarise the history of the IoT and why it is difficult to find a definition (2). The third sub-section will provide the most accurate description possible of the IoT paradigm structure, which underpins the concept of the modern smart-home and the domestic IoE(3) . The methodological *caveats* are well known: in this part there is a description of how this technology works by focusing more on technical aspects than law and policy ones. In any case, there will be explanations of the most technical

terms and processes in the footnotes for non-technical experts. The fourth subsection will try to explain why, despite the fact that the IoT is already more than twenty years old, the smart home is not yet a widespread habitation scheme (4). Another part of the chapter focuses on the possible classification criteria of the IoT for the house (5). The third and last part of the chapter will try to outline the recent developments of IoT technology, listing and explaining the different technologies which will respectively make the IoT more decentralised (Edge Computing), its way of operating more intelligible (application of blockchain and DLT), and more environmentally sustainable (the Green IoT or GIoT) (6).

2. History of the IoT and struggles for a definition

The IoT is not a new technology, as it is about 23 years old[32]. Nevertheless, I think it is useful to provide a summary of the history of how the IoT developed and how it is connected with the smart home. The first connected object ever made was a computer-connected Sunbeam Toaster. Its creators, John Romkey and Simon Walter Hackett took on this unusual challenge in a world without Wi-Fi by relying simply on TCP communication protocols [33]. This object was presented at the Interop conference in 1990[34]. However, it was Kevin Ashton who put forward the idea of creating a possible "things" specification of ubiquitous computing, a concept described by Mark Weiser in 1991. According to the latter, computer technology had to be everywhere and yet almost invisible[35]. The fact that Ashton called this technology "Internet of Things" in 1999 was more of an accident than a part of a specific plan: this new technology of things and sensors seemed promising from the beginning as it was possible *i)* to control it, in order not to waste energy; *ii)* to know when to replace an object, and *iii)* to calculate loss in advance [36].

Despite the fact that it is quite clear that the everyday functioning of the original IoT mostly meant embedding short range mobile transceivers[37] into a

[32] However, some scholars consider Nikola Tesla to be the first to think about this technology. Tesla imagined that connected devices would be simpler and would "*convert the Earth into a brain*". Guido Noto La Diega, *Internet of Things and the Law. Legal Strategies for Consumer-Centric Smart Technologies* (London: Routledge, 2022), 11.

[33] In short, TCP stands for Transmission Control Protocol. It is a standard that ''*[...] defines how to establish and maintain a network conversation by which applications can exchange data*". Ben Lutkevich, "What is Transmission Control Protocol (TCP)?," *TechTarget*, October 2021, Accessed 31 January 2023, https://www.techtarget.com/searchnetworking/definition/TCP .

[34] John Romkey, "The Toast of the IoT. The 1990 interop Internet toaster", *IEEE Consumer Electronics magazine* 6, 1 (2017): 116-119 http://doi.org/10.1109/MCE.2016.2614740 . Shristi Deoras, "First Ever IoT Device – The Internet Toaster", *Analytics India Magazine*, August 5, 2016, https://analyticsindiamag.com/first-ever-iot-device-the-internet-toaster/ .

[35] Mark Weiser, "The Computer for the 21st Century," *Sci-Am* (1991).

[36] Kevin Ashton, "That 'Internet of Things' Thing," RIFID Journal, 22 June 2009, https://www.rfidjournal.com/that-internet-of-things-thing .

[37] Transceiver in electronics indicate a component which can be a receiver and transmitter at the same time. Katie Terrell Hanna, "Transceiver," *TechTarget*, September 2021, https://www.techtarget.com/searchnetworking/definition/transceiver .

growing array of objects[38], both technical experts and legal communities are still at odds over finding a satisfactory definition for the IoT. For some, the presence of Internet and Things in the same expression will always be a sign this technology is at the intersection between products and things[39]. Some authors believe it more important to highlight the things that are connected through different technologies such as Radio Frequency Identification (RFID), Wireless Sensor Networks (WSN), Bluetooth, Near Field Communication (NFC), Long Term Evolution (LTE)[40] technologies. Sometimes, on the contrary, the focus of the definition is the internet infrastructure and technologies, such as in the ITU[41] definition which describes the IoT as "[*a*] *global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies*"[42]. The EU agency for cybersecurity, ENISA[43], describes the IoT as "*a cyber-physical ecosystem of interconnected sensors and actuators, which enable intelligent decision making*"[44]. This definition focuses on the relationship with the environment and on the distinctive objects that make the IoT work, such as sensors and actuators (more description *infra*).

Furthermore, one could also take a more abstract and a philosophy-of-information approach and understand that the IoT is the first ever made *onlife* application. This is apparent if we consider the fact that the *onlife* experience blurs the boundaries between the online and the offline world[45]. As far as legislative definitions of the IoT are concerned, an explicit one has still not been established in the EU[46]. However, this does not mean that the IoT is not expanding or that it does not have any importance in EU policies. In brief, what almost all these definitions are lacking is actually the consequences that the IoT has on people's data. The functioning and scope of each piece of the IoT will be explained shortly *infra* but, solely for clarity, one of the technical characteristics

[38] Debasis Bandyopaday and Jaydip Sen, ''Internet of things: Applications and challenges in technology and standardization,''*Wireless Personal Communications*, 58, 1 (2011): 50 https://dx.doi.org/10.1007/s11277-011-0288-5; At the beginning of IoT development, the proprietary technology by EPC Global and GS1 had started a technology relying on the Electronic Product Code (EPC) which contained embedded RFID tags. A supply of the information contained in the RFID tag was saved by linking and cross linking this information through the help of an Object Naming Service (ONS), a distributed tree-like domain name system to store the information of the object also on an external server. More on this in Rolf H. Weber, "Internet of Things- Need for a New Legal environment?'', *Computer Law and Security Review*, 25, 6 (2009): 522-527, https://dx.doi.org/10.1016/j.clsr.2009.09.002.

[39] Debasis Bandyopaday and Jaydip Sen, ''Internet of things: Applications and challenges in technology and standardization,''*Wireless Personal Communications*, 58, 1 (2011): 50, https://dx.doi.org/10.1007/s11277-011-0288-5.

[40] Abhishek Khanna, and Sanmeet Kaur, "Internet of Things (IoT), Applications and Challenges: A Comprehensive Review,'' *Wireless Personal Communications*, 114, 2 (2020): 1688, https://doi.org/10.1007/s11277-020-07446-4.

[41] ITU stands for International Telecommunications Union, https://www.itu.int/en/Pages/default.aspx .

[42] ITU, *Recommendation ITU-T Y 2060 (6/2012) Overview of the Internet of Things*, (Geneva, 2012), 1, https://handle.itu.int/11.1002/1000/11559.

[43] ENISA is the European Union Agency for Cybersecurity, see https://www.enisa.europa.eu/ .

[44] Enisa, *Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures* (ENISA, 2017), 18.

[45] The Onlife Initiative, '' The Onlife Manifesto,'' *The Onlife Manifesto: Being Human in a Hyperconnected Era*, Luciano Floridi (Cham, Heidelberg, New York, Dodrecht, London: Springer, 2015), 7.

[46] The only document mentioning the IoT but not defining it is the Free Flow of Data Initiative and the Data Act, see 1.1 in Chapter III. Whereas in the US there is a federal definition of IoT. See more in 1.2, Chapter V.

of the IoT that will be relevant for the liability discussion is that IoT objects function and are able to perform better thanks to data processing. Data can be non-personal, as in not referable to an identified or identifiable person, such as the temperature of a smart fridge; or it could be personal, such as the fingerprint to unlock one's smart phone. Basically, data processing is what makes home IoT devices more special than the traditional ones.

In order to perform and to react, the IoT object needs a considerable quantity of data from its user(s) both for commercial and non-commercial purposes. That is why more recently, in 2020, the Von der Leyen Commission announced initiatives that will create a better infrastructure for the IoT: with increased cybersecurity and a tool to ensure a safe 5G network[47], which should increase the potential use of the IoT, to a safe space in which to store data for several kinds also of IoT gathered data, such as the Industrial IoT and the Healthcare IoT[48].

The success of the IoT in terms of investments depends on the simple idea of connecting everyday objects to the Internet at an acceptable price (at least while the price and availability of rare earth materials are still within an acceptable range) and an acceptable speed[49]. Furthermore, there is a large variety of different fields in which this technology can be employed to automatise, monitor and control processes[50] . This was already quite clear from the start of development of this technology[51]. In addition, there are also other technological factors that should be factored into the investment in this technology. Apart from the strides made in increasing computational power, which makes data processing easier and faster, Reyes and Salam explain that there are at least twelve reasons why the IoT has been expanding in this way. Among these reasons there is, on the one hand, the fusion between Internet Technology (IT) and Operational Technology (OT) and, on the other hand, the transformation

[47] "COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Secure 5G deployment in the EU - Implementing the EU toolbox, COM/2020/50 final," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:0050:FIN.

[48] "COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A European strategy for data COM/2020/66 final," EUR-Lex, Accessed 31 January 2023., https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066, 20.

[49] The latest estimate of the value of the IoT market in 2020 according to Mordor Intelligence globally is $ 761.4 billion and is expected to reach 1.39 trillion by 2026. See Mordor Intelligence, INTERNET OF THINGS (IO) MARKE- GROWTH, TRENDS, COVID 19 IMPACT AND FORECASTS (2021-2026) https://www.mordorintelligence.com/industry-reports/internet-of-things-moving-towards-a-smarter-tomorrow-market-industry. According to a McKinsey report, the value of the IoT has not been consistently exploited, as foreseen by the same McKinsey 5 years earlier. Nevertheless, it also shows some estimates concerning the economic value of the Internet of Things adoption in 2030. The home applications are worth between 440 and 880 billion dollars, distributed among the labels of chore automation, energy management and safety and security. Michael Chui, Mark Collins and Mark Patel, IoT "Value set to accelerate through 2030: Where and how to capture it?," McKinsey Digital, 9 November 2021, https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/iot-value-set-to-accelerate-through-2030-where-and-how-to-capture-it.

[50] See the supra note 17 McKinsey Digital.

[51] Debasis Bandyopaday and Jaydip Sen, ''Internet of things: Applications and challenges in technology and standardization, ''*Wireless Personal Communications*, 58, 1 (2011): 50 https://dx.doi.org/10.1007/s11277-011-0288-5;

brought on by the phenomenon of digital convergence[52]. This last phenomenon means that not only are some kinds of technology "hybridizing" other kinds of technology (such as the IoT and AI) but also people and the external environment as a whole. In brief, this means that the end result will really be the Internet of Everything, the IoE[53], which takes into consideration not only devices, but data and people as well.

This fosters a deeper fusion between IT (internet technology) and OT, but, given the problems of data traffic and space, current solutions concerning cloud computing are being slowly changed by augmenting the computational power at the edge of the objects. These last two aspects can be seen as a further explanation of Moore's law[54].

3. The IoT structure

From a technological point of view, we have described the IoT as the group of technologies and instruments (sensors, actuators, electromagnetic waves, but also a distant infrastructure of servers and a cloud system) that is able to create a connected environment with the help of embedded software and through constant monitoring and ubiquitous sensing techniques.

From a technological point of view, Reyes and Salam see the IoT as being divided into 4 different layers:

"1) devices (things)
2) network (infrastructure transporting data)
3) service platform (software connecting the things with applications)
4) applications" [55]

[52] The reasons according to which the IoT has experienced such a development according to Rayes and Salam are the following: "1) current fusion of IT (internet technology) and OT (operational technology; 2) astonishing introduction of creative internet based businesses; 3) mobile device explosion;4) social network explosion; 5) analytics at the edge; 6) cloud computing and virtualisation; 7) technology explosion (meaning that also computational power was made cheaper and accessible to normal people; 8) digital convergence and transformation (digital convergence being the coming together of different technologies in a single device, hence the transformation;9) enhanced user interfaces;10) fast rate of IoT technology adoption; 11) rise of security requirements12) the non-stop of the Moore's law[this element is debatable]". Ammar Reyes and Samer Salam, *Internet of Things From Hype to Reality The Road to Digitization* (Springer Nature Switzerland, 2019, 2nd ed), https://link.springer.com/book/10.1007/978-3-319-99516-8 .

[53] See definition in Chapter I.

[54] Moore's law takes the name of the American Engineer Gordon Moore and as he foresaw already in 1965 that the number of transistors for silicon chips doubles every year. However, this law has recently been criticised as it suggests an idea of technological development that is endless, whereas the resources for this planet are finite even for ITC technologies. It appears already that from a computational point of view technology has been experiencing a standoff as computational powers in microchips and CPUs seems to have peaked. For a more informed discussion see David Rotman, "We are not prepared for the end of Moore's Law," *MIT Technology Review*, February 24, 2020, Accessed 31 January 2023, https://www.technologyreview.com/2020/02/24/905789/were-not-prepared-for-the-end-of-moores-law/.

[55] Ammar Reyes and Samer Salam, *Internet of Things From Hype to Reality The Road to Digitization* (Springer Nature Switzerland, 2019, 2nd ed) 7.

Other tech experts might add an additional layer (5-layer model, including a business or transport layers)[56] or even up to 7 layers[57]. These latter models tend to be over-complex and are not really functional if we are interested in understanding how this technology is relevant for applications concerning EU private law.

Hereinafter, the following conversion nomenclature for the smart house will be adopted. It is based more on a functional approach divided into layers: 1) devices-perception/physical layer; 2) network and communication layer 3) processing-computation layer 4) applications layer.

It is essential to understand that all part of the smart home environment relies on data provided through the inhabitant's input. However, in order to understand how the IoT paradigm functions, it is essential to know that it works through different logical steps and different layers, each of which is specialised in one single function that has data collection, management and analysis as its objectives.

The most concise description through which it will be possible to reconstruct the IoT paradigm in the home as described in the methodology is the following. The inhabitant of the house (or someone who is approaching the house) moves, expresses a voice command, or more simply gives an input that is collected and registered by sensors. There are many types of sensors that can have different functions. They constitute the perception-layer[58]. This layer is also called data-collecting layer or physical layer, according to the importance of either the data or devices for classification. Secondly, the *stimulus/ i* acquired by the physical layer is/are sent as analogue data to the IoT service Network through a gateway (communication layer). Then the physical input which has been transformed into a digital format is sent to the Fog (eventual) and the Cloud where the proper data processing is performed (processing layer). Finally, the original data as processed in the Cloud/proprietary network is used to automate several functions in the smart home (application layer) [59]. The reply/reaction to the initial stimuli is sent back, first as data and then as an electric signal to different components of the perception layer: the actuators.

3.1. The technological side: sensors

[56] Pallavi Sethi and Smruti R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications," *Journal of Electrical and Computer Engineering* (2017) https://dx.doi.org/10.1155/2017/9324035.
[57] Nallapeni Manoji Kumar and Pradeep Kumar Mallick, "The Internet of Things: Insights into the building blocks, component interactions, and architecture layers," *Procedia Computer Science* 132 (2018): 109-117 https://dx.doi.org/10.1016/j.procs.2018.05.170.
[58] Bako Ali and Ali Ismail Awad, "Cyber and Physical Security Vulnerability Assessment for IoT-based smart homes," *Sensors* 18,3 (2018):817 https://dx.doi.org/10.3390/s18030817 .
[59] Ammar Reyes and Samer Salam, *Internet of Things From Hype to Reality The Road to Digitization* (Springer Nature Switzerland, 2019, 2nd ed) 7. Enzo Tartaglione, *IT for beginners* , Lecture materials, University of Turin, September- October 2020.

The Instrument Society of America defines a sensor as a device that provides a usable output to a specified measure[60]. It acquires a physical parameter and converts it into a signal suitable for processing (e.g., optical, electronical, mechanical). In a way, the sensor is the physical interface that allows the IoT paradigm to function as it is. It has been argued that without a sensor it would be impossible to carry out smart automation in the house.

The need for different types of sensors is due to a phenomenon called ubiquitous sensing[61], which is a derivation of ubiquitous computing[62] and has led to the concept of the ubiquitous home, which can be understood as a domestic environment based on a network of intelligent sensors[63]. The philosophy for home sensors is to create a space, in our case the smart home, that is reactive to the behaviours of the inhabitant and that is able to analyse them in order for the environment to be the most customised possible[64].

Since the beginning of studies in the smart living or ambient intelligence field, houses have been seen as the perfect environment where technological changes that allowed telemedicine or healthcare services to be implemented, for instance through wearables devices connected with RFID (Radio Frequency Identification) technology that comprise sensors. Nowadays there is a growing trend according to which sensors in the smart home are used not only to sustain elderly people or people with disabilities[65] but also to deal with climate-change and to make the living more sustainable[66], in compliance with the SDG requirements[67].

Although there are now many sensors that can make a house smart[68], and they are generally easily available to the general public, there is no uniform classification of these objects.

---

[60] "Introduction to Sensors and Transducers," *Electronics Hub. Projects, Tutorials, Reviews and Kits*, February 19, 2019, https://www.electronicshub.org/sensors-and-transducers-introduction/.

[61] Ubiquitous sensing is defined as the ambient "where a network of sensors, integrated with a network of processing devices deals with a rich yet multi-modal stream of data". Dan Ding, Rory A. Coper, Paul F. Pasquina and Lavinia Fici-Pasquina, "Sensor technology for smart homes," *Maturitas* 69,2 (2011):131-136, https://dx.doi.org/10.1016/j.maturitas.2011.03.016 . For more see also Fernando V. Paulovich, Maria Cristina F. De Oliveira and Osvaldo N. Oliveira Jr, "A Future with Ubiquitous Sensing and Intelligent systems," *ACS Sens*, 2018, 1433-1438 https://pubs.acs.org/doi/pdf/10.1021/acssensors.8b00276 and Stephan Sigg, Kai Kunze and Xiaoming Fu, "Recent Advances and Challenges in Ubiquitous Sensing", *PIEE* (2015) https://arxiv.org/abs/1503.04973 .

[62] Mark Weiser considered ubiquitous computing as the last phase of the evolution of computing when we, as subjects would not mind technology as it is overwhelming in our life (1991). Mark Weiser, "The Computer for the 21st Century," *Sci-Am* (1991).

[63] Tatsuya Yamazaki, "The Ubiquitous Home," *International Journal of Smart Home* 1,1 (2007): 17-18.

[64] Dan Ding, Rory A. Coper, Paul F. Pasquina, Lavinia Fici-Pasquina, "Sensor technology for smart homes," *Maturitas* 69,2 (2011):131-136, https://dx.doi.org/10.1016/j.maturitas.2011.03.016 . https://doi.org/10.1016/j.maturitas.2011.03.016.

[65] Cristian Gómez Portes et al., "Automatic Generation of Customised Exergames for Home Rehabilitation on physical mobility constraints and key performance indicators," in *Intelligent Environments*, Carlos Iglesisas et (Amsterdam: IOS Press,2020): 29, https://dx.doi.org/10.3233/AISE200020.

[66] Tiago Serrenho, P. Bertoldi, *Smart home and appliances: State of the art. Energy, Communications, Protocols and Standards*. (Luxembourg: JRC, 2019).

[67] UNDP. *Sustainable Development Goals*. Accessed 31 January 2023. https://sdgs.un.org/goals.

[68] 30 sensors according to Samsung. See Home Stratosphere, "Smart Home Sensors," May 18, 2020, Accessed 31 January 2023, https://www.homestratosphere.com/smart-home-sensors/.
8 according to IBM. "Sensors and Smart Home." *IBM*. December 15, 2016, Accessed 31 January 2023, https://www.ibm.com/blogs/internet-of-things/sensors-smart-home/

Sensors can be categorised according to their different **physical** properties, **environmental** and **economic** costs. Physical properties that need to be considered include latency, accuracy, precision, and the predisposition to deteriorate (such as the tendency to be corroded). Sensors can also be categorised according to how the input is perceived. There can be **direct sensing** acquired through binary sensors[69] as in pressure sensors or contact switches. Direct sensing can also be carried out through video cameras, which are considered "high-content sensors"[70]. Another direct sensing method is the use of RFID. This is based on tagging each object with a unique identifier and, when using a RIFID reader, the tag responds [71]. There are two types of RIFID tags: *i)* passive tags that are not energetically autonomous and are generally attached to the object; *ii)* active tags which instead are energetically autonomous[72]. There are other kinds of direct sensors that do not rely on binary systems and offer more specific information. They might be measuring temperature and keeping a log of acoustic signals. Then, the last group according to this classification is made of the so-called **infrastructure mediated systems** which cost generally less, and require the installation of one or a few sensors in the house that reduces the complexity of the overall deployment. However, they are not efficient from the perspective of the detail of activity it provides [73]. Furthermore, sensors can be categorised depending on their **function**: it can be surveillance and security of the house (e.g., webcams, smart doors); smart home management (smart lights, thermostats, fridges, washing machines) but also entertainment for the inhabitants and guests (smart televisions, stereos, augmented reality devices etc.).

Moreover, there is a classification that follows the **specialisation of the different areas of the house** (e.g., kitchen, bedroom, living room, bathroom) but this does not seem quite as practical to use as some smart appliances can be found in different environments at the same time.

One of the most advanced sensors that will be increasingly used in the smart home is the APS (active pixel sensors). This is a more advanced light sensor that produces a signal that is properly conditioned and is transformed in encoded images[74] . There are also ultra-sonic sensors that are specialised in converting acoustic waves into electric signals[75]. They are cheap and come in a

[69] Which simply detects the state of an object or movement with a single digit 1 or 0. Din (2011)p.131
[70] Dan Ding, Rory A. Coper, Paul F. Pasquina and Lavinia Fici-Pasquina, "Sensor technology for smart homes," *Maturitas* 69,2 (2011), https://dx.doi.org/10.1016/j.maturitas.2011.03.016 ,132
[71] *Ibid.*
[72] *Ibid.*
[73] Dan Ding, Rory A. Coper, Paul F. Pasquina and Lavinia Fici-Pasquina, "Sensor technology for smart homes," *Maturitas* 69,2 (2011), https://dx.doi.org/10.1016/j.maturitas.2011.03.016 ,133
[74] Enzo Tartaglione, *IT for beginners*, Lecture materials, University of Turin, September- October 2020.
[75] Enzo Tartaglione, *ibid*., 2020. Stefano Meroli, "Design and implementation of Active Pixel Sensors (APS)," Stefano Meroli. Life of an Engineer at CERN, Accessed 31 January 2023, https://meroli.web.cern.ch/lecture_activepixelsensors.html.

huge variety[76] Particle detectors are also increasingly used sensors and will be mainly used to monitor the levels of air pollution or smoke[77].

However, it is noteworthy that sensors are already acquiring considerable potential through Edge Computing technology [they are also enjoying lower prices], that will allow devices (the "edge" of the IoT system) to become more powerful from a computational point of view. This will rely on smart sensors, that are enriched by a tiny, simplified computing system. In short, this technology allows more computational power to be stored at the edge of the connected system.

3.2. The technological side: actuators

Technically, the actuator is *"[…] a type of motor that is responsible for controlling or taking action in a system. It takes a source of data or energy"*[78]. Actuators allow the practical side of home automation. They consist of "*nodes, […], of a network that are connected with each other through wireless technology*"[79]. After the input has been transformed into data and analysed at cloud level, actuators are part of the device that receives data back under the form of an electrical command. This electronic input orders the actuator to react. As a result, the home environment will meet the conditions wanted by the inhabitant of the house. The most known on the market are the so-called linear actuators or lifting columns.[80] Physically, a new generation of actuators is already becoming quite well known: these are add-on devices that help in the automation process, for instance by pushing, pulling objects after a response from the cloud is sent back as a reaction to a first stimulus. It is interesting to witness a new season of actuators that can be connected with smart assistants in order to manage the house, thus reducing the problems of interoperability[81]. It is believed that, with the increase of Edge Computing Technology (more *infra*), it will also be possible for actuators to store the logs of their activities in the physical device.

---

[76] Enzo Tartaglione, *ibid.* 2020. Stefano Meroli, "Design and implementation of Active Pixel Sensors (APS)," Stefano Meroli. Life of an Engineer at CERN, Accessed 31 January 2023, https://meroli.web.cern.ch/lecture_activepixelsensors.html.

[77] Enzo Tartaglione, *ibid*., 2020. Stefano Meroli, "Design and implementation of Active Pixel Sensors (APS)," Stefano Meroli. Life of an Engineer at CERN, Accessed 31 January 2023, https://meroli.web.cern.ch/lecture_activepixelsensors.html.

[78] Ammar Reyes and Samer Salam, *Internet of Things From Hype to Reality The Road to Digitization* (Springer Nature Switzerland, 2019, 2nd ed), 82 https://link.springer.com/book/10.1007/978-3-319-99516-8 See also Peter Marwedel, *Embedded System Design. Embedded systems, foundations of cyber-physical systems, and the Internet of Things* (Springer Cham, 2018) 185-186 https://link.springer.com/book/10.1007/978-3-319-56045-8.

[79] Sebastian Dengler, Abdalkarim Awad and Falko Dressler , "Sensor Actuator Network in Smart Homes for Supporting Elderly and Handicapped people Conference: 21st International Conference on Advanced Information Networking and Applications (AINA 2007)", Workshops Proceedings, Volume 2, May 21-23, 2007, Niagara Falls, Canada, *IEEE*, https://dx.doi.org/10.1109/AINAW.2007.325 .

[80] TiMOTION, The role of electric actuation in smart homes, Accessed 31 January 2023, https://www.timotion.com/en/news/news_content/news-and-articles/comfort-motion/the-role-of-electric-actuation-in-smart-homes?upcls=1481189409&guid=1529663363.

[81] For example see Designboom, "smartians" actuators turn your everyday products into smart devices, Accessed 31 January 2023, https://www.designboom.com/technology/frolic-studio-smartian-actuators-turn-your-everyday-products-into-smart-devices-11-21-2018/

3.3. The technological side: the gateway

The gateway is either a device or a virtual appliance that *"...offers local processing and storage solutions as well as the ability to autonomously control field devices based on data input by sensors"*[82]. It fulfils three main functions: *"(1) collecting and aggregating information from the devices, (2) on-site filtering and simple correlation of collected information (3) transferring correlated data to the network layer and (4) taking action on devices*"[83].

With more and more smart objects becoming available to consumers, internet protocols and interoperability at large are becoming a cause of fragmentation that makes it difficult for smart objects and appliances to function and to communicate with each other. The IoT was originally called Machine to Machine Communication (M2M) because what was initially sought after was a way to enable human-intelligent agent interaction. However, agent-agent interaction also had to be developed in order to reach a better degree of automation, hence, M2M communication. At the moment, on the market there are six main types of smart home gateways[84], with different interoperability sets and different ranges from one another. Technologically, the answer to this problem would be to create a single Internet Protocol (at least for the house) to have better interoperability.

3.4. The technological side: the cloud

The Cloud can be described as a part of the so-called "far from the user" and "immaterial" processing layer, where all the operations of data analysis and the elaboration of the output to send back to the smart object are elaborated. The US National Institute of Standards and Technology (NIST) describes it as "[…] *a model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers* […]) *that can be rapidly provisioned and released with minimal management effort or service provider interaction*"[85]. The Cloud contributed not only to a

[82] Juan Pedro Tomás, "What is an IoT gateway?"*Enterprise IoT insights,* 2017, Accessed 31 January 2023, https://enterpriseiotinsights.com/20170517/internet-of-things/20170517internet-of-thingswhat-iot-gateway-tag23-tag99 . For an in depth presentation of several gateway frameworks and cyber security issues for IoT see Sunil Chevuru et al, *Demystifing Internet of Things Security. Successful IoT Device/Edge and Platform Security Deployment*. (New York: Springer Apress Open, 2020), 133-146.
[83] Ammar Reyes and Samer Salam, *Internet of Things From Hype to Reality The Road to Digitization* (Springer Nature Switzerland, 2019, 2nd ed), p.183
[84]In Lin-An Phan and Taehong Kim's work there is the mention of the most important gateways for the home)Samsung Smart Things 2) Apple Homekit 3) Wink Hub 4) VeraSecure 5) Homey 6) Home Seer. (tabe 1). See Lin-An Phan and Taehong Kim, "Breaking down the compatibility problem in Smart Homes. A Dynamically Updatable Gateway Platform," *Sensor* 20,10 (2020): 2873, https://dx.doi.org/10.3390/s20102783. Mozilla is now working on a getaway for the house that should work in a way that is more privacy compliant within the bigger Framework of the Project Mozilla IoT Web of Things. Mozilla, Web of Things, website, Accessed 31 January 2023, https://iot.mozilla.org/gateway/.
[85] Peter Mell and Timothy Grance for NIST, *The NIST Definition of Cloud Computing* 2011, 2. Accessed 31 January 2023, http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf.

dematerialisation of resources, thus reducing archiving and storing costs[86], but also made it possible to save enormous quantities of data from material damage, with the possibility of accessing them remotely at any moment in time[87].

Nowadays, because of the underpinning process of miniaturisation investing technology, some scholars are also discussing the potential of mobile cloud computing[88]. Mobile cloud computing is also the main infrastructure underpinning the design of contemporary home IoT[89].

In recent years, cloud providers also started applying data analytics techniques to the data they received, especially if the company offering the cloud storage service was also offering other services for companies (such as software services). Through the use of these new algorithmic-based techniques, it was possible to increase the revenues by finding patterns in consumers' and clients' behaviours, by adopting more efficient strategies. However, the use of the data stored in clouds also caused problems as processing was carried out almost exclusively through complex algorithms, causing issues which were also under the scrutiny of competition law experts[90] and, where personal data were involved, creating data protection law concerns[91] .

4. The smart home and the IoT paradigm

The IoT is a flexible and adaptable technology. One of the applications is the smart home, meaning a domestic connected environment (4.1). The functioning of the IoT does not change: the smart home is made up of the same components that have just been described (sensors, actuators, gateway and cloud). In the last ten years, consumers have started seeing the multiplication of either new objects for their homes which connected them to the Internet, such as the Amazon Dash button (no longer sold)[92], voice assistants such as Google

[86] Stefano Quintarelli, *Capitalismo immateriale* (Torino: Bollati Boringhieri, 2019), 26-33. Hereinafter, Quintarelli.
[87] Quintarelli ibid.
[88] Mobile computing is defined as *"[…] an infrastructure where both the data storage and data processing happen outside of the mobile device. Mobile cloud applications move the computing power and data storage away from mobile phones and into the cloud, bringing applications and MC to not just smartphone users but a much broader range of mobile subscribers"*. Hoang T. Dinh, et al. "A survey of mobile cloud computing: architecture, applications, and approaches," *Wireless Communications and Mobile Computing* 13 (2013):1597-1611, https://onlinelibrary.wiley.com/doi/epdf/10.1002/wcm.1203.
[89] Ronald Leenes and Silvia De Conca, "Artificial intelligence and privacy- AI enters the house through the Cloud" In *Research Handbook on the Law of Artificial Intelligence*, Woodrow Barfield, Ugo Pagallo (Chelthenam: EE publishing 2018), 285-306.
[90] See *ex multis* the seminal work of Ariel Ezrachi and Maurice E. Stucke, "Artificial intelligence & collusion: When computers inhibit competition," *University of Illinois Law Review* 5 (2017): 1775-1810.
[91] W. Kuan Hon, C. Millard, I. Walden, "The problem of "personal data" in cloud computing: What information is regulated? the cloud of unknowing," *International Data Privacy Law* 1,4 (2011):211-228, https://dx.doi.org/10.1093/idpl/ipr018.
[92] In Germany, this button was also considered to be not compliant with the EU Consumer Rights Directive EU/2011/83 as it did not give consumer a meaningful comparison with other products to choose from except the ones selected by Amazon and because it did not give a clear indication about the payment after clicking the button to get a certain object. See in Christoph Busch, "Does the Amazon Dash Button Violate

Home, Amazon Alexa-Echo, Siri, Cortana and Bixbi, or old objects have been made "smart" (windows sills, dishwashers, ovens etc…). However, it is important to point out that there is not yet an agreement on what a smart home is and, secondly, it is not yet a widespread way of living because of policy, sociological issues and technological shortcomings (4.2).

4.1. Is the smart home still to arrive?

The first ideas concerning the smart home, picturing it as the *non plus ultra* of luxury and comfort, date back to the beginning of the 1930s, when automation was connected to the availability of electricity[93]. The modern conception of the smart home is much younger, as it relies instead on the paradigm of ubiquitous computing, as announced by Mark Weiser in 1991 (Ubicomp), as a technology that was able to disappear, but was extremely pervasive[94]. Gradually, the original Ubicomp idea evolved into the idea of spreading computing in everyday life under the name of "everyday computing", an expression created by Abwod and Mynatt ten years after Weiser's Ubicomp paradigm[95]. One year after the creation of the term "everyday computing", Edwards and Grinter narrowed down their analysis on the challenges that were still to be solved in order to create ubiquitous computing at home and for the first time elaborated the concept of smart homes, as *"…domestic environments in which we are surrounded by interconnected technologies that are, more or less, responsive to our presence and actions"*[96]. They assumed that if the home had to become a ubiquitous environment on a large scale, this would occur through a piece-meal process. At that time (and also nowadays), connected home experiments were part of university research projects in most cases[97]. Grinter and Edwards postulated that if smart homes had to become a widespread model of living, there were seven different challenges to overcome: i) that the smart home unfolding was happening in a piece-meal way that could create confusion; ii) that interoperability of all the systems had to be guaranteed; iii) the fact also that there was not one single administrator of the

EU Consumer Law? Balancing Consumer Protection and Technological Innovation in the Internet of Things," *Journal of European Consumer and Market Law* 2(2018): 78-80.

[93] Yolande Strengers, *Smart Energy Technology in Everyday Life. Smart Utopia* (Palgrave Macmillan, 2013) https://dx.doi.org/10.1057/9781137267054 : 23-25.

[94] Mark Weiser, "The Computer for the 21st Century," *Sci-Am*,1991.

[95] Gregory D. Abwod and Elizabeth D. Mynatt, "Charting Past, Present, and Future Research in Ubiquitous Computing," *ACM Transactions on Computer-Human Interaction*, 7,1 (2000): 29.

[96] Keith Edwards W., and Rebecca E. Grinter, "At Home with Ubiquitous Computing: Seven Challenges," in *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* Gregory D. Abwod, Barry Burmitt and Steven Shafer (Springer Verlag Berlin Heidelberg, 2001) 2201: 256 https:/dx./doi.org/10.1007/3-540-45427-6_22 .

[97] For university smart homes smart of project see the Georgia University one in *Ibidem* and see also, for Japan, Tatsuya Yamazaki, "The Ubiquitous Home," *International Journal of Smart Home* 1,1 (2007): 17-18. Instead, for private projects, already at the end of the 1970s this idea of Ubicomp had transferred to some home automation protoypes called the Xanadu houses Roy Mason and Lane Jennings built three "computer homes" in different parts of the US at the end of the 1970s which showcased some computer-powered automated solutions. Read more in Xanadu Houses, *Wikipedia*, Accessed 31 January 2023 https://en.wikipedia.org/wiki/Xanadu_Houses which were both touristic attractions but also the centre of extensive critical remarks to a utopia in which technology would solve all the problems of the post-industrial society. For an extensively structured critic see Kevin Robins and Mark Hepworth, "Electronic spaces: new technologies and the future of cities,"*Futures* 20,2 (1989): 155-176.

smart home system was seen as a challenge technically, even before legally; iv) also the design of the object had to adapt for domestic use; v) privacy was seen as an important social implication that had to be kept in mind by IoT objects creators; vi) reliability of the technological system and the decision of how "smart" the home had to be[98].

Two different things have happened since the definition of a smart home as given by Grinter and Edwards, that they had not thought about. On the one hand, for a long time, the "smarting" process passed through electricity rather than computing, starting from the creation of smart grids and efficient ways to distribute energy[99]. It then passed through some identifiable objects such as smart thermostats in the house which helped to not waste energy.[100] According to Darby, at first, technical experts and policy makers did not have the wide diffusion of the smart home as one of their objectives, as energy efficiency and energy saving were the primary objectives to have in a connected home[101].

On the other hand, with the increase of computational power, it was easier to build the IoT paradigm. From that moment on, private law scholars and practitioners started to show more interest as there was more focus on the objects and the intelligent systems that would integrate tangible and usable everyday consumer products, as they were more readily connected to traditional issues of contractual, extra-contractual, strict and product liability law.

With regard to the EU approach to the smart home and its connection to environment sustainability, there are still quite a few obstacles to overcome, although there have been several policy efforts in recent years on this theme. As far as the EU approach to smart buildings and smart homes is concerned, there is still a division between energy law/policy aspects the consumer law (private law) ones in the EU. When discussing energy policy/law, the EU was working on smart homes even before the European Green Deal of 2019[102]. In fact, the previous European Commission had started an ambitious project to renovate buildings and make them more environmentally sustainable. As a consequence, in 2018 the EU Parliament amended the existing directives on building energy

[98] Keith Edwards W., and Rebecca E. Grinter, "At Home with Ubiquitous Computing: Seven Challenges," in *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* Gregory D. Abwod, Barry Burmitt and Steven Shafer (Springer Verlag Berlin Heidelberg, 2001) 2201: 256 https://dx.doi.org/10.1007/3-540-45427-6_22 .

[99] According to Darby, at first, technical experts and policy makers did not primarily have the objective of the wide diffusion of smart homes because of its environmental sustainability potential but it was a welcome second effect. Sarah J. Darby, "Smart technology in the home: time for more clarity," *Building Research and Information* 46,1 (2018): 142 Sarah J. Darby, "Smart technology in the home: time for more clarity," *Building Research and Information* 46,1 (2018): 142 https://dx.doi.org/10.1080/09613218.2017.1301707.

[100] Nazmiye Balta-Ozkan, Oscar Amerighi and Benjamin Boteler, «A comparison of consumer perceptions towards smart homes in the UK, Germany and Italy: reflections for policy and future,» *Technology Analysis and Strategic Management* 26,10 (2014): 1176-1195, https://dx.doi.org/10.1080/09537325.2014.975788 .

[101] Sarah J. Darby, "Smart technology in the home: time for more clarity," *Building Research and Information* 46,1 (2018): 142 Sarah J. Darby, "Smart technology in the home: time for more clarity," *Building Research and Information* 46,1 (2018): 142 https://dx.doi.org/10.1080/09613218.2017.1301707.

[102] "COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS The European Green Deal, COM/2019/640 final," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2019%3A640%3AFIN.

efficiency and building energy performances[103]. The proclamation of the European Green Deal was the start of activities connected to the so-called Renovation Wave, which was supposed to help buildings become more energy saving and ecologically sustainable by making them "greener" and refurbishing them, in order to reach 0 net emission by 2050[104]. Furthermore, within the Renovation wave, the first edition of the New Bauhaus Initiative took place in 2021: this was a competition for innovators, architects and citizens to find solutions for sustainable living (both urban and domestic) and to discover and employ new materials[105].

Instead, with regard to the EU consumer policy for the home, what drove the last years in terms of legislative output was the digital transformation of the economy, which will be described better in chapter III. In this sub-section there will be a discussion solely regarding the environmental efforts to make the IoT for the home "greener". Under the Juncker commission, the results of the REFIT procedure led to a profound renovation[106]. Among other initiatives, the approvals of the directives EU/771/19 (SDG)[107] on the sale of goods, including the ones with digital elements, and EU/770/19 on certain aspects concerning contracts for the supply of digital content and digital services (DCDS)[108], were particularly relevant for the smart home, for instance. The objective was to make consumer law and data protection more technologically up to date and coherent. However, the GDPR[109], which is also applicable when domestic IoT objects deal with personal data, mentions neither environment nor sustainability and commentators observed that for consumer law, the "silo" approach to legislation and regulation that had been criticised in the past had also remained the same in these legislative acts[110].

---

[103] Directive (EU) 2018/844 of the European Parliament and of the Council of 30 May 2018 amending Directive 2010/31/EU on the energy performance of buildings and Directive 2012/27/EU on energy efficiency (Text with EEA relevance) PE/4/2018/REV/1*OJ L 156,* 19.6.2018 p. 75–91, "EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L0844.

[104] "COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A Renovation Wave for Europe - greening our buildings, creating jobs, improving lives COM/2020/662 final," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0662.

[105] New Bauhaus Initiative, Accessed 31 January 2023, https://europa.eu/new-european-bauhaus/index_en.

[106] Evelyne Terryn, "The New Consumer Agenda : A Further Step Toward Sustainable Consumption?" (2021) 10 1.

[107] "Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC (Text with EEA relevance.) PE/27/2019/REV/1*OJ L 136, 22.5.2019,* p. 28–50," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32019L0771. Hereinafter DCDS.

[108] "Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services (Text with EEA relevance.) PE/26/2019/REV/1*OJ L 136, 22.5.2019,* p. 1–27," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32019L0770. Hereinafter SDG.

[109] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)*OJ L 119, 4.5.2016, p. 1–88*

[110] Evelyne Terryn, "The New Consumer Agenda: A Further Step Toward Sustainable Consumption?", *Journal of Consumer and Market Law* 10,1 (2021): 1-3.

The only common thing between the Consumer law and Energy law policy was that the concept of smart home is not mentioned once. Despite the lack of an official legislative or policy definition about the smart home, Sovacool and Furszyfer Del Rio compared and contrasted the most influential definitions of smart homes which, despite having been drafted for energy policy purposes, are neutral enough to also be used in future documents about the consumer and data protection law aspects of the smart home. In fact, in all of them the house is described as a sum of parts which can or cannot be part of an energy supply system[111]. To summarise, the smart home is an interconnected environment which relies on the IoT today and Internet of Everything (IoE) tomorrow, and whose purpose is to make the life of its inhabitants better by also pursuing the objective of environmental sustainability[112].

According to the vision of Edwards and Grinter and to the last definition of smart home above, the smart home should be something that is positive and therefore it should have a widespread application, at least in the EU. However, the present features of our homes and our consumer habits are influencing domestic technology and not *vice versa*. At the moment, if we follow the indications of Edwards and Grinter, we do not yet live in a ubiquitous/smart home. We are in an "accidental smart home" phase: some people might be starting to rely on sustainable resources of energy through which they are self-sufficient thanks to home-automation. Many others might not. With different percentages according to the MS, European consumers express interest in having technology that might simplify their life and be respectful of the environment[113]. Further, the investments in this market of domestic IoT are considerable as is the impact on consumers' data of this technology. That is the reason why the EU Commission has carried out a sector inquiry into the consumer IoT[114].

Some of the reasons for which people should be attracted by the idea of the smart home include simplifying life and better management of their

[111] Table 2 mentions eleven prominent definitions of the smart home. The first one by Lutlof is from 1992 and focuses more on integrated services and communications systems that ensure a secure functioning of the home. Aldrich (2003) mentions the element of information technology, but the scope is different as it focuses on the necessity for technology to be reactive to the inhabitants, which is similar to the definition of De Silva et al. (2021). Balta Ozakan instead insists on the fact that the communication network of the house can be controlled and monitored also from afar (2014). For Hargreaves and Wilson (2017) instead the most important element is data collection for the better management of the home. Strengers and Nicholls (2017) definition instead mentions for the first time the IoT as a residual category of the smart house, less characterised from the home ICT and automated appliances. Shin et al.'s definition (2018) is centred on the need of the house to react and provide services to the occupants. Also Gran-Hanssen and Darby (2018) instead made the aim to give service a focus but without the mention of monitoring and control unlike Shin et al. (2018). Benjamin K. Sovacool, Dylan D. Furszyfer Del Rio, "Smart home technologies in Europe: A critical review of concepts , benefits , risks and policies," *Renewable and Sustainable Energy Reviews* 120 (2019): 109663 https://dx.doi.org/10.1016/j.rser.2019.109663

[112] This is the process through which we defined smart home in chapter I about methodology.

[113] For instance, Italians are in theory in favour of having smart objects to save energy. In 2021 there have been 2.7 million euros worth of smart gas management devices installations, and over 4.8 milion smart metering devices. Instead, the proper smart-home sector has witnessed a downside compared to 2020 (the investment was of just 505 million euros, -5% compared to 2020). Osservatorio Internet of Things, *L'Internet of Things alla prova dei fatti: il valore c'è e si vede!* (Milano: Politecnico di Milano 1863 School of Management and osservatori.net digital innovation, 2021),12-13.

[114] Press release European Commission: Antitrust: Commission launches sector inquiry into the consumer Internet of Things (IoT) https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1326 .

home. From an equality point of view, a home that is able to help with the necessities of elderly people who are still autonomous but need to be assisted, and also the possibility for technology to increase the quality of life of people with disabilities is certainly something to aspire to[115]. However, there are policy, social and technological reasons for the lack of smart homes at present, which will be explained in the following subsection.

4.2. Why the smart home is not yet here to stay

As explained before, there are both social and technological reasons why smart homes are not a common, widespread reality yet.

There are social factors that need consideration. Several models indicate conditions that make a technology truly successful. The most renowned theory is the one concerning the Perceived Usefulness of Technology and the Perceived Ease of Use of Technology[116].

However, Balta Ozakan and others, in their seminal article on the social barriers to the adoption of smart homes, also outlined that that there were differences in the priorities of the groups of people who participated in the study. In fact, the group that could be defined as "experts" and the group of "normal people" (homeowners and generally consumers) expressed different views on home automation. In general, technical experts tended to focus more on the stability and reliability of the system both as an infrastructure and as a provider of services which could span from private entertainment for the home inhabitant to specific health needs [117]. Contrary to that, and most surprisingly even before the Cambridge Analytica scandal, common users were more concerned about the aspect of consumer policy and privacy in addition to the cost these technologies might entail[118]. It could be for this reason that there may have been a lower demand than during recent years. This is also reflected at the level of solutions: for a long time, there was no certainty for EU consumers that they could rely on the existing EU consumer legislation to extend it to objects with digital elements. Moreover, as it will be clarified further, there was no EU legislation directly or indirectly applicable to domestic IoT until 2019. Only in that year there was the publication of the two directives on the sale of digital goods and supply of digital contents that could be applicable to IoT objects (see *infra* chapter III)[119]. Finally, as explained in Chapter IV, only a pandemic such as COVID-19 could

---

[115] Dimitar Stefanov, Zeungnam Bien and Won-Chul Bang, "The smart house for older persons and persons with physical disabilities: Structure, technology arrangements, and perspectives," *IEEE Transactions on Neural Systems and Rehabilitation Engineering* (2004); Andrew Sixsmith and Gloria Gutman, *Technologies for Active Ageing* (New York, Heidelberg, Dodrecht, London: Springer 2013).

[116] Fred D. Davis, "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Technology," *MIS Quarterly* 13,3 (1989):319-340.

[117] Nazmiye Balta-Ozakan et al, " Social barriers to the adoption of smart homes," *Energy Policy* 63 (2013):367-371, http://dx.doi.org/10.1016/j.enpol.2013.08.043.

[118] Nazmiye Balta-Ozakan et al, " Social barriers to the adoption of smart homes," *Energy Policy* 63 (2013):367-371, http://dx.doi.org/10.1016/j.enpol.2013.08.043.

[119] More precisely, both the SDG and DCDS could be applied starting from 1st July 2022.

have speeded up digital literacy processes and the progressive “smarting” of homes.

The technical problems are more structured. They concern both the external telecommunication structure on which the IoT is based and also the way in which IoT objects are able not only to react to their owners but also to other IoT objects.

In order for the IoT to have better performance, low latency is key. Latency is the delay in the input-response time lapse. The lower the latency is, the faster it is to accomplish data operations which are crucial for domestic IoT. That is why having a 5G network grants a better performance for IoT objects as it has a higher bits-rate transmission, a bigger capacity, a lower latency time, a consistent QoS (Quality of Service) and the possibility to deliver device intelligence services[120]. Since 2020, the IoT issue has been part of the new EU Commission plan for the next five years in different documents and deployment of the 5G network was included in the necessary steps to reach the Digital Decade within the framework of the State of the Union Speech. The importance of IoT technology and the infrastructure that is required to be competitive was stressed through the release of the 5g Toolkit and the enactment of the Cybersecurity Code[121].

Despite the first initiatives on the 5G of the EU Commission date back to 2013[122], the full deployment of this technology is still not complete[123], both for difficulties in structuring PPPs (Private Public Partnerships) which help in the roll-out of this technology[124] and also because of widespread environmental sustainability concerns about this technology[125]. These concerns persist despite applications of 5G, such as energy harvesting, should help making this technology more environmentally sustainable[126].

The second technological problem concerns interoperability. Interoperability is the technical capacity for Internet technologies to communicate

---

[120] Sabrina Sicari, Alessandra Rizzardi, Alberto Coen-Porisini, “5G In the Internet of Things era: An overview on security and privacy challenges,” *Computer Networks* 179 (2020): 107435; and Kinza Shafique, Bilal Khawaja, Farah A. Sabir et al., “Internet of things (IoT) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5G-IoT Scenarios,” *IEEE Access* 8 (2020): 23027.

[121] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast)Text with EEA relevance. PE/52/2018/REV/1 *OJ L 321, 17.12.2018*, p. 36–214, http://data.europa.eu/eli/dir/2018/1972/oj.

[122] European Commission, “5G,”Accessed 31 January 2023, https://digital-strategy.ec.europa.eu/en/policies/5g.

[123] European Commission, “5G Observatory Quarterly Report 13 Up to October 2021,” Accessed 31 January 2023. https://5gobservatory.eu/wp-content/uploads/2021/11/5G-Obs-PhaseIII_Quarterly-report-13_final-version-11112021.pdf .

[124] Lithuania and Portugal still lack any kind of deployment of 5G (see previous study).

[125] Gianluca Quaglio, *Environmental Impacts of the 5G. EPRS study.* (Brussels: European Union 2021) 1-149.https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690021/EPRS_STU(2021)690021_EN.pdf.

[126] Sudhir K. Routray., and K.P. Sharmila, “Green Initiatives in 5G,” in *Proceeding of IEEE - 2nd International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics, IEEE - AEEICB 2016* (Chennai,India, 2016) : 619-620 https://dx.doi.org/10.1109/AEEICB.2016.7538363.

with one another. The IoT in reality is made of different technologies and they all need to communicate with each other for a smart environment to function. In order to achieve this result, standards are needed to codify how interoperability can take place between two or more objects of the same specific environment. Standards are rules and know-how on how to create safer and better products and processes, new technologies included. They are generally created by Standard Setting Organisations (SSOs) or Standard Developing Organisations (SDOs) which can have a national, regional and international outreach. Especially international and regional SSOs or SDOs are important in information technologies because they generally gather the best experts of the sectors and provide the state-of-the-art standards. There are SDOs and SSOs for IoT objects already present and they have mostly either an international or a European outreach[127].

SDOs and SSOs in IoT technology give rise to two particular issues which are connected respectively with IP/ competition law and private law. The first one concerns the relationship these standards have with patented technologies. Generally, for an IoT such as a smart phone there are a myriad of patents employed[128]. However, standards that are essential to the development of that specific technology could also contain patents. Due to both their essentiality and the fact of belonging to a standard they are called Standard Essential Patents (SEPs). If innovators want to proceed and need a definite standard containing patents they have to ask for a fee which should be released under Fair Reasonable and Non Discriminatory terms (F/RAND licences)[129].

In the past, there were cases, both in the US and UK but also in the EU[130], in which SEP patent holders would ask for ludicrously high fees or, alternatively, they would not even mention that an innovation was patented and subsequently sued the innovator (which could also lead to a vertical abuse of dominance in competition law[131]). Nowadays, “patent wars” in the telecommunications sector have decreased in intensity but this does not mean that concerns over interoperability and fair competition to develop better and safer products are resolved. Controversies like the ones just mentioned might also take place with reference to the domestic IoT, as smart objects are built on almost the same technological paradigms which were at the origin of these technological disputes. The Staff Accompanying Report of the sector inquiry into the Consumer Internet of Things describes concerns over IoT standardisation in its eighth part. In

[127] Francesca Gennari, “Standard Setting Organisations for the IoT: How To Ensure a Better Degree of Liability?,” *Masaryk University Journal of Law and Technology* 15,2 (2021): 162-166, https://dx.doi.org/10.5817/MUJLT2021-2-1 .
[128] In the US the agency RPX estimated that there were at least 250,000 patents in order to build a smart-phone. Patent Progress, “Too many patents,” Accessed 31 January 2023, https://www.patentprogress.org/systemic-problems/too-many-patents/.
[129] Jorge Contreras, “Origins of FRAND Licensing Commitments in the United States and Europe,” in *The Cambridge Handbook of Technical and Standardization Law. Competition, Antitrust, and Patents*, Jorge Contreras (Cambridge: Cambridge University Press, 2017), 149-169. https://dx.doi.org/10.1017/9781316416723.012 .
[130] Chryssoula Pentheroudakis and Justus Baron, *Licensing Terms of Standard Essential Patents. A Comprehensive Analysis of Cases* (Luxembourg: JRC, 2017) https://dx.doi.org/10.2791/32230.
[131] Judgment of the Court (Fifth Chamber) of 16 July 2015, *Huawei Technologies Co. Ltd v ZTE Corp. and ZTE Deutschland GmbH* (Huawei). Case C-170/13, ECLI:EU:C:2015:477.

particular, there is a problem concerning the multitude of said SDOs/SSOs often producing almost interchangeable standards (interoperability ones included). Moreover, there is no clarity concerning the IPR policies of each SDO/SSO, not to mention the overall costs of the standardisation process that only multinational firms are able to sustain financially[132]. Furthermore, the lack of transparency about how a standard is set and how SEPs are chosen[133] can be a cause of concern for people advancing their own innovations as part of a standard, but also it can have repercussions on the quality and the safety of the final result of the standard in general.

In addition, international standards *per se* are not mandatory, unless they are officially adopted in technical regulations by each MS in Europe. The problem is that because of the prestige these SSOs/SDOs have, IoT producers, manufacturers or innovators will abide by these standards which might turn out to be the cause of damage, as they could create or cause the IoT object to malfunction. To date in the US, no technological SDOs/SSOs has been held liable[134].

There have not been many cases in the EU involving the liability deriving from faulty standards but there are at least two famous examples that can help in understanding what the consequences would be in EU law if an interoperability IoT standard were to be considered defective. They did not concern IoT technological standards but they reflect two methods in risk management that are not unusual to EU law. The first one is derived from the CJEU judgment *James Elliott Construction*[135] which is of interest because of its application of Regulation 1025/2012 on harmonised standards[136]. Being an instrument of co-regulation between the EU and MS, the regulation on harmonised standards establishes that the Commission dictates general criteria for developing technical standards, and the European SDOs/SSOs (generally

[132] "Commission Staff Working Document. Accompanying the document REPORT FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT Final-Report- Sector inquiry into consumer Internet of Things (COM(2022)19 final) , Brussels, 20.1 2022, SWD(2022) 10 final. 89". EUR-Lex, Accessed 31 January 2023. Commission Staff Working Document Accompanying the Document REPORT FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT Final report- Sector inquiry into consumer Internet of Things, SWD/2022/10 final" EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022SC0010&qid=1653852206944, 106-110 Hereinafter, Staff Working Document- Report on the Consumer IoT.

[133] Staff Working Document- Report on the Consumer IoT, 106-110.

[134] Paul Verbruggen, "Tort Liability for Standards Development in the United States and the European Union," in *The Cambridge Handbook of Technical Standardization Law. Further Intersections of Public and Private Law* in Jorge Contreras (Cambridge: Cambridge University Press 2019), 60-88 https://dx.doi.org/10.1017/9781316416785.005.

[135] "James Elliott Construction Limited v Irish Asphalt Limited, Case C-613/14,." EUR-Lex, Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62014CJ0613. Hereinafter *James Elliott Construction*.

[136] "Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council Text with EEA relevance, *OJ L 316, 14.11.2012, p. 12–33,*" EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32012R1025 .

CEN, CENELEC and ETSI) develop these standards which are later published in the Official Journal of the EU (OJ). The OJ standard is a harmonised EU standard. In *James Elliott,* the case involved a EU harmonised standard concerning the production of cement which turned out to be faulty. The CJEU established that it had competence on the matter given that the standard was published as an EU act. However, neither the regulation nor the judgment states more about the hierarchy of harmonised standards in the EU law, nor does the judgment regarding the justiciability of those standards if they are defective.[137]

The second scenario is the one where there are intermediate private/public-private bodies, called Notified Bodies (NB) trusted both by the EU Commission and the MS, which have auditing and certification powers over standards of objects whose use could be intrinsically risky and dangerous. The mission of these NB is to check and certify whether the product actually meets all the prescribed product safety requirements. This model was firstly exemplified by the Medical Devices Directive (MDD)[138], now repealed by the Medical Devices Regulation (MDR)[139]. The contents of these legislative acts will be further explained in Chapter III, V, and VI but, at present, the focus is on the entities that had to certify that the medical device was compliant with the conformity requirements and on the liability of the certification/auditing bodies, the NB. Under the MDD, there was no explicit mention of liability (caused by negligence or contract) of the NB. The only idea of liability was expressed by the possibility (therefore not an obligation) for the NB to take out civil liability insurance. In *Schmitt,* the CJEU established that negligence by a notified body (NB) in auditing the correct application of standards to build high risk medical devices did not prevent MS from adding further liability schemes, provided that these would not disrupt the logic and creation of the Internal Market[140] as liability was not explicitly mentioned in the directive. To date, the only EU jurisdiction that applied this principle was the French *Cour de Cassation*[141] in a class-action which involved several women who, like the plaintiff in *Schmitt*, had discovered that they had defective breast implants from the same medical devices manufacturer, PIP, and wanted compensation from the NB, TÜV France and TÜV Germany. The French *Cour de Cassation* applied the Schmitt judgment, explaining that both NB were

[137] Carlo Tovo, "Judicial Review of Harmonised Standards: Changing the Paradigms of Legality and Legitimacy of Private Rulemaking under EU Law," *Common Market Law Review* 55 (2018):1187-1216. More on this issue from a liability point of view can be found in Chapter V, first section.
[138] "Council Directive 93/42/EEC of 14 June 1993 concerning medical devices *OJ L 169, 12.7.1993, p. 1–43*," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31993L0042.
[139]"Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Text with EEA relevance.) *OJ L 117, 5.5.2017, p. 1–175*," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R0745.
[140] "Elisabeth Schmitt v. TÜV Rehinland LGA Products GmbH, Case C-219/15." EUR-Lex, Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/GA/ALL/?uri=CELEX:62015CJ0219. Hereinafter, *Schmitt.* See also Anna Wallerman, "Pie in the sky when you die? Civil liability of notified bodies under the Medical Devices Directive: *Schmitt*," *Common Market Law Review* 55 (2018): 265-278.
[141] Cour de Cassation, Première Chambre Civile, Arrêt n° 616 du 10 octobre 2018 (17-14.401), ECLI:FR:CCASS:2018:C100616.

considered to be negligent as they had a general duty of surveillance over the medical devices manufacturer.

The main problem in these two instances is that the private body does not have any contractual relationship with the person who has suffered damages (generally a consumer and/or a patient). Hence, in both cases (*Schmitt* and *James Elliott Construction*) the solution for the plaintiff would be to apply tort liability, and, if the MS traditional legal history allows it, also some contractual liability applications. More on this will be discussed in chapter III, IV and V.

5. Functional taxonomies for the IoT in the home

Up to this point, the focus of the chapter has been the explanation of the IoT and smart-home history and architecture, together with the social and technical reasons why the smart home is not yet a common reality for EU citizens.

In order to shift the focus to a legal analysis of liability in the smart home, it is necessary to try to provide a summary of the many different products and services that IoT/future IoE objects might offer in the smart home. This is not an exhaustive list, of course, but it is based on an internet search for products and services delivered at home[142]. It is possible to list different categories from this data. These categories are based on different perspectives.

5.1. The novelty criterion

The first intuitive criterion is based on whether or not the object was already present among the objects we use as consumers. For instance, smart TV sets, smart stereo systems, smart light bulbs, smart ovens, smart dishwashers, smart washing machines, smart pillows, smart phones and smart watches are only upgrades of objects that we were using even before the Internet. At the same time, there are new objects that did not exist before such as cleaning robots or integrated voice assistants.

Generally, well-established electronics producers developed their own smart domestic appliance product lines. They also generally all develop a smartphone application to control the device and often allow interoperability for voice commands, generally with Google Home and Alexa, and, less frequently with Apple and Bixbi (Samsung)[143].

The tendency to develop *ad hoc* applications and software for “new” objects also seems consolidating: it happened for the best-known voice assistants (Alexa

[142] This search is carried out on Google by browsing the sites of the best known domestic object IoT providers: Amazon Alexa and home appliances, Google home and Nest, Philips Hue, Samsung Smart Things thing, IRobot, Somfy, Lutron, WeMo, Ecobee, Tuya, Sonos, Miele, General Electric, AEG and Whirlpool.

[143] This is the case for GE, Whirlpool, Bosch, AEG

and Google Home and, to a certain degree BixBi from Samsung), which laid out the basics to create a smart environment by either producing new appliances (such as Amazon Smart Bulbs) or by acquiring already existing brands specialised in domotics, as Google did by acquiring Nest, the one-time leading smart thermostat manufacturer on the market[144]. Other producers of existent house and personal electronic objects also created software to automatise their own appliances (such as Smart Things, by Samsung or Alexa by Amazon and Google Home by Google). Some of them also make it possible to control non-electronic devices such as precious objects or pets. This allowed - especially with SmartThings- the creation of tags to put on the collar of a pet or on the surface of a valuable object such as eyeglasses[145].

The main positive aspect of this method is that it makes it easier to separate the many home IoT objects into just two groups. The disadvantage of this approach is that it does not necessarily help in finding the law applicable to these objects in the event that damage is suffered.

5.2. The autonomy criterion

Another criterion is not so much based on the pre-existing nature of a specific domestic IoT object, but on its autonomy. This criterion seems straightforward to apply if we consider that the majority of home IoT objects cannot technically be considered as AI systems at the present moment, as the algorithms that are employed by the IoT objects are very rarely part of the software within the object itself. They instead cooperate with the object from the cloud. From this aspect, IoT objects could be better compared to robots. In this case, labelling label the different kinds of IoT objects according to the autonomy criterion may be justified. This is what Guerra does when talking about robots and also including IoT objects[146].

- Level 0: *No Autonomy*. A smartphone app that provides a 'smart music accompaniment (like playing with an orchestra) while the inhabitant is practicing an instrument at home or a mobile app that enables instruments to be tuned.
- Level 1: *Robot Assistance*. Home IoT Assistance: the object is simply a mechanical guide assisting the home inhabitant (e.g., a multi-tasking cooker)
- Level 2: *Task Autonomy*. The IoT is autonomous solely for specific tasks (the inhabitant programs the cleaning time for a small cleaning robot)
- Level 3: *Conditional Autonomy*. An IoT generates options in relation to one of its functions, but the home-inhabitant will have to choose. For instance, a smart microwave can recognise the kind of food (frozen chicken meat) and suggest the de-frost function followed by a pre-cooking phase.

[144] Alexei Orsekovic, " Google to acquire Nest for $3.2 billion in cash," *Reuters*, January 13, 2014, https://www.reuters.com/article/us-google-nest-idUSBREA0C1HP20140113.
[145] Samsung, SmartThings, Accessed 31 January 2023, https://www.samsung.com/it/apps/smartthings/.
[146] Giorgia Guerra, *La sicurezza degli artefatti robotici in prospettiva comparatistica. Dal cambiamento tecnologico all'adattamento giuridico*. (Bologna: Il Mulino, 2018), 97.

- Level 4: *High Autonomy*. The IoT object takes a decision under human supervision. For instance, smart thermostats analyse the data concerning the temperature outside and inside the house to adjust, but the inhabitant can always change the output. Another example are the empathic-interactive robots for kids which have a high level of autonomy.
- Level 5: *Full Autonomy*. The human does not play any role. At the moment, this level is not reached in any of the areas of research involving new technologies[147].

The main positive aspect is that the classification divides the IoT into different groups but does not help in identifying which laws might be applied. In addition, many might disagree that the IoT should be compared to robots directly. As mentioned, the AI component in the IoT objects is rapidly changing its way of working and may completely transform them into consumer applications which mainly rely on AI for their functioning than on the original IoT paradigm. Hence this classification might not be as useful for legal purposes in the future.

5.3. The EU Commission classification of Consumer IoT

The already cited Staff Working Document- Report on the Consumer IoT also gave a rather refined classification of consumer IoT objects based on market segments. For each of these segments, a group of stakeholders had to fill in the EU Commission survey on consumer IoT. The previously mentioned market segments are: *i)* manufacture of smart home devices; *ii)* provision of voice assistants; *iii)* manufacture of wearable devices and *iv)* provision of consumer IoT services (such as creative content services)[148]. This division is thought to detect possible competition law infringements according to Articles 101 and 102 of the TFEU. However, this classification is useful as it is also accompanied by an attempted definition. For instance, the report only contains the expression “voice assistants”, not smart assistant or other similar expressions that may be quite simple to find on the Internet. The definition of voice assistant given in the report , on the other hand,sees the voice assistant more as a “[…] *voice-activated pieces of software* […]”[149] that also happens to have a physical container. This is probably inspired by the guidelines on voice assistants published by CNIL, the French Data Protection Authority (DPA) as it describes a voice assistant as“ *[…] une application logicielle offrant des capacités de dialogue oral avec un utilisateur en langage naturel […].*”[150]. Furthermore, it may be useful to bear the market segmentation adopted by the Commission in mind, as it divides the market into two groups: the producers of IoT as goods (smart home and wearable devices) and the providers of services (through voice assistants and, in general, services that can range from entertainment, to security and control). The fact that these

[147] Giorgia Guerra, *La sicurezza degli artefatti robotici in prospettiva comparatistica. Dal cambiamento tecnologico all’adattamento giuridico*. (Bologna: Il Mulino, 2018), 97.
[148] Staff Working Document- Report on the Consumer IoT, 20 (24).
[149] Staff Working Document- Report on the Consumer IoT, 20 (25).
[150] (Translation from the author) “A software application which offers spoken language skills to a user in natural language. CNIL, *À votre écoute. Exploration des enjeux éthiques, techniques et juridiques des assistants vocaux*, (CNIL; Paris, 2020),12.

groups also coincide with the division between goods and services in consumer law can also help provide a better understanding of which models of liability have been adopted so far and whether they are effective[151]. The only negative aspect is that this categorisation seems to be more directed at competition issues for obvious reasons.

5.4. Mixed functions of domestic IoT objects

It is possible therefore to divide the objects according to their core function. At the moment, several groups can be identified

- coordination of a diverse range of appliances: smart remote controllers and plug-ins; regulation of light, temperature, voice assistants, smartphone apps;
- security: video-cameras, smart locks, tags with GPS facility for locating pets or precious objects, security systems which coordinate locks, gates and garages of the house;
- health: connected gym devices, wearables such as smart watches or bracelets, smart pillows, air purifiers, smart rings, heart and glucose monitors, empathic/ interactive robots for kids and elderly people
- cleanliness and hygiene: small cleaning robots, dish-/washing and drying machines
- entertainment and learning: smart TVs, smart stereo systems, exergames or Virtual Reality (VR) games through the use of special headsets or other devices (prompt guitar or tennis racket) with pressure and grip sensors.

At the start of this paragraph, it was specified that the functions in this list are the core functions of the objects cited. I point this out as one of the qualities of domestic IoT objects is that they often combine several functions in a single device. The primary function of a smart-watch is to keep its user informed about the time and weather, but it can also have health-monitoring functions. For instance, one can keep track of the steps taken per day, and heart-rate frequency.

Therefore, a further layer of this classification is: mono-function and multifunction objects. Certainly, the ones that seem to be more interesting are the domestic IoT that mix consumer with healthcare functions. The IoT for healthcare market is set to expand due to the effect of the Covid-19 pandemic and the issues connected to ageing populations (see Chapter IV and VI). It is likely that most visits, rehabilitation programmes, and monitoring services will be increasingly carried out remotely. Most likely, hospitals will need to be operational not only for COVID-19 patients, but also women in labour, emergencies and other medical treatments that cannot be performed at home. It should also be borne in mind that, according to the Commission's IoT inquiry report, voice assistants are becoming the major gateways to all the other appliances in the house. It will be interesting to understand what the implications would be when a smart exergame that is provided by a hospital for a home rehabilitation programme is made interoperable with a consumer-commercial voice assistant.

[151] More on this in Chapters III, IV and V.

EU law can easily be applied here, as it is based on the division on goods and services. Moreover, it is possible to rely on the CJEU *Uber*[152] judgment when there is uncertainty about whether a function is the main one or not. In particular, in *Uber,* it was demonstrated that a teleological approach is the right one to analyse the function of an object or service.

6. Future technological perspectives

The IoT is far from being technologically perfect. There are several technical defects which characterise the IoT, and consumer/home IoT in particular. Firstly, even modern IoT objects for the home need an excessive amount of data to be compliant with privacy and data protection data regulations worldwide[153]. Secondly, the over-production of data (or data-deluge) risks producing problems of data traffic within the Internet structure if it relies excessively on external clouds. This creates problems such as the overcrowding and slowing down of the Internet structure possible. Thirdly, the fact that this paradigm relies too much even today on a centralised paradigm - mainly on the cloud - makes it also more vulnerable at its periphery: in fact, the cybersecurity of IoT objects is not as developed as it should be, especially for consumer objects that are in general less expensive than proper healthcare or industrial IoT devices, such as the most popular IoT for the home. Lastly, the current IoT model relies on rare earth materials as components which are becoming more and more scarce[154], alongside the recent semiconductors scarcity[155]. It seems however that some other technologies can change the IoT paradigm from both within (3.1 and 3.3) and without (3.2).

6.1. Fog and Edge computing

As a consequence of IoT development, huge quantities of data have been produced in recent years, giving origin to a phenomenon called "*data deluge"*[156].

---

[152] A teleological and qualitative analysis on the freedom to provide intermediation services and transport services can be found in §§ 37-42 "Asociación Profesional Elite Taxi v Uber Systems Spain, SL, Case Case 434/15 ," EURlex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62015CJ0434 .

[153] IoT Analytics estimated that in 2021 there would be 12.3 billion active IoT endpoints and that by 2025 IoT connections would amount to 27 billion. Satyajit Sinha, "State of IoT 2021: Number of connected IoT devices growing 9% to 12.3 billion globally, cellular IoT now surpassing 2 billion," *IoT Analytics*, 22 September 2021, Accessed 31 January 2023, https://iot-analytics.com/number-connected-iot-devices/.

[154] This also explains why the EU has created the European Raw Market Alliance and a European Rare Earths Competency network to ensure recovering and availability of this materials. European Commission, Internal Market (webpage), "*Rare earth elements, permanent magnets and motors*", Accessed 31 January 2023, https://ec.europa.eu/growth/sectors/raw-materials/areas-specific-interest/rare-earth-elements-permanent-magnets-and-motors_en .

[155] Maria Grazia Attinasi et al, "The semiconductor shortage and its implications for euro area trade, productions and prices,". European Central Bank webpage, Accessed 31 January 2023, https://www.ecb.europa.eu/pub/economic-bulletin/focus/2021/html/ecb.ebbox202104_06~780de2a8fb.en.html .

[156] As a proportion think that "Five exabytes of data have been generated from the dawn of humanity to 2003. Now this much data is generated every two days". Ammar Reyes and Samer Salam, *Internet of*

From a technical point of view, this factor loaded the Internet infrastructure with more data, thus augmenting the traffic overall. From a structural point of view, an uncontrolled rise in Internet traffic can lead to technical shortcomings that could have long-lasting consequences on businesses and the structure of the Internet in general[157].

That is why, in 2014, CISCO first elaborated the foundation of the Fog Computing paradigm[158]. For the first time it allowed: *i)* the most time-sensitive data at the network edge, close to where it is generated, to be analysed *ii)* a very short latency time, (meaning that the capacity of reaction starting from IoT data is in the order of a few milliseconds); *iii)* data for the cloud to be selected and sent for longer storage[159]. This would allow the infrastructure not to be overloaded and businesses to have more control and possibilities to analyse fruitful data captured by the IoT. In practical terms, this is done by augmenting the computational capability of the device and by creating a further transparent layer between the devices and the cloud, called fog.

Technically, "*Fog computing, or in short Fog, refers to a platform for integrated compute, storage and network services that are highly distributed and virtualised. This platform can extend in locality from IoT end devices and gateways all the way to Cloud data centres but is typically located at the network edge. Fog augments Cloud computing and brings its functions closer to where data is produced (e.g., sensors) or needs to be consumed (e.g., actuators)*"[160].

The fog layer relies on a consequence of Moore's law, which connects the evolution of computing and storage technologies[161].

Originally, Edge computing is an older paradigm than fog computing (the first theorisation was made in 2009) and is structured in two alternative ways: either there is a creation of small cloudlets (small clouds similar to the Wifi Hotspots) that are accessed through user equipment (devices) or there is an increase in the device's computational power[162]. As for cloud computing, Edge computing now also has a mobile version too called Mobile Edge Computing which allows smart objects to improve the QoS (Quality of Service) and QoE

Things From Hype to Reality The Road to Digitization (Springer Nature Switzerland, 2019, 2nd ed), 156 https://link.springer.com/book/10.1007/978-3-319-99516-8.

[157] Jun-Ho Hu and Yeong-Seok Seo, "Understanding Edge Computing: Engineering Evolution with Artificial Intelligence," *IEEE Access* 7(2019):164229, https://dx.doi.org/10.1109/ACCESS.2019.2945338.

[158] CISCO*, Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are. White Paper* (2015):1-6, Accessed 31 January 2023, https://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/computing-overview.pdf.

[159] CISCO, *Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are. White Paper* (2015):1-6, Accessed 31 January 2023, https://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/computing-overview.pdf.

[160] Ammar Reyes and Samer Salam, *Internet of Things From Hype to Reality The Road to Digitization* (Springer Nature Switzerland, 2019, 2nd ed), 155 https://link.springer.com/book/10.1007/978-3-319-99516-8.

[161] Ammar Reyes and Samer Salam, *Internet of Things From Hype to Reality The Road to Digitization* (Springer Nature Switzerland, 2019, 2nd ed), 156 https://link.springer.com/book/10.1007/978-3-319-99516-8.

[162] Pavel Mach, Zdenek Becvar, "Mobile Edge Computing: A Survey on Architecture and Computation Offloading," *IEEE Communications Surveys and Tutorials* 19,3 (2017):1628-1630, https://dx.doi.org/10.1109/COMST.2017.2682318 .

(Quality of the user's experience)[163]. To understand Edge Computing, one has to know a bit more in detail about how the data cycle in home IoT work. I will briefly reiterate what was stated. After the sensorial inputs are collected at the physical/device layer through sensors on the objects, data are then transformed into digital signals and are sent to a gateway which has the function of selecting the data and sending them to the cloud or proprietary network. However, traffic on the web has increased in an astonishing way during the last ten years. Even before privacy, structural concerns interested the technical experts: it was apparent to many that the Internet infrastructure based on the cloud model could not last forever. Because of such infrastructure concerns, Edge Computing was developed further. The idea is actually quite simple. If computational power cannot exceed a certain threshold, nothing actually prevents objects or parts at the edge of the entire cloud system from becoming more computationally powerful, thus maintaining an overall balance. This will mean that small computational units will be hosted by more devices that will be able to process and analyse data, but also to keep a log of all the operations performed at the edge by the IoT object. The problem of sending all data to the cloud (which it maybe is outside the EU) would not exist anymore.

6.2. Distributed Ledger technologies and Blockchain for the home

The IoT has been the paradigm for "smart" communications of objects since the early years of the 2000s. Despite that, it has been known for a while that the security level and integrity of IoT (especially domestic application) can be easily breached. One of the main liabilities is that, overall, the IoT is quite a centralised system. At both ends, at the edge of it and in the immateriality of the cloud, there are basically no techniques to protect the data from being stolen by hackers. It goes without saying that the problems are even greater if third party data is involved in a data breach. But centralisation is not the only structural problem with IoT in general, and home IoT in particular. Also, the low battery and traditionally low computational power (including memory) made security and data protection challenges more apparent in IoT objects which are also called constrained devices. It is true that Edge Computing can be quite a game changer in augmenting the computational strength of even home IoT objects but some efforts have also been made in order to apply some low-weight cryptography (cryptography is a method of developing techniques and protocols to prevent a third party from accessing and gaining knowledge of the data from private messages during a communication process) which can adapt better to the specificities of the IoT[164].

That is why technical and legal experts are wondering whether Distributed Ledger Technologies (DLTs) and Blockchain can serve to correct traditional structural IoT deficiencies. Distributed ledgers are *ipso facto* de-centralised

[163] Ibid.
[164] Ankur Lohachab, Anu Lohachab and Ajay Jangra, "A comprehensive survey of prominent cryptographic aspects for securing communication in post-quantum IoT networks", *Internet of Things* 9 (2020): 100174, https://dx.doi.org/10.1016/j.iot.2020.100174.

structures, which permanently fix transactions made by users working collaboratively. However, the kind of cryptographic techniques used by DLT (symmetric and asymmetric functions together with hash functions) require a considerable quantity of power to perform communication between simple IoT objects. Some questions therefore persist about whether a full implementation of DLT and Blockchain protocols in IoT objects would give problems in terms of scalability. Most technical experts are convinced that there must be specific DLT/Blockchain protocols to make the IoT more secure[165]. That is why there are already experimentations of protocols such as IOTA[166], Chain of Things[167], Riddle &Code[168]; Modum.io[169].

The advantages could be quite sensible, not only from the cyber security and privacy angles, but also from the point of view of liability. Transparency in transactions can explain better what happened and who caused damage. There is currently no way to find out easily through the cloud system. Furthermore, in the event of damage, the IoT could register all that happened and ascertain almost exactly who or what was at fault for causing the damage. Still the applications for blockchain/DLT IoT are not yet widely commercialised as they consume a huge amount of energy and they are not able to perform tasks as fast as the cloud paradigm would allow, hence they are not scalable.

6.3. The new Green IoT (GIoT)

The Green IoT (hereinafter GIoT) is a promising new field of automation engineering also combined with material research, whose objectives is to decentralise the IoT cloud-based structure and make it ecologically more sustainable. The structure of the GIoT is practically the same as described before, but what changes is the effort in reducing network wastes of energy. Some ways to reach this objective are, for instance, creating new techniques for routing data and bringing them closer to the user and using new materials that are known for their non-toxicity and that could in principle be recycled[170]. This promising field is

---

[165] Abraham Ayeba Alfa et al., "Blockchain technology in IoT systems: current trends, methodology, problems, applications, and future directions," *Journal of Reliable Intelligent Environments* (2020), https://dx.doi.org/10.1007/s40860-020-00116-z ; Daniel Minoli and Benedict Occhiogrosso, "Blockchain mechanisms for IoT security," *Internet of Things* 1-2 (2018):1-13, https://dx.doi.org/10.1016/j.iot.2018.05.002.

[166] Bilal Shabandri and Piyush Maheshwri, "Enhancing IoT Security and Privacy Using Distributed Ledgers with IOTA and the Tangle," in *2019 6th International Conference on Signal Processing and Integrated Networks (SPIN) Enhancing* (2019) 1069-1075, https://dx.doi.org/10.1109/SPIN.2019.8711591.

[167] Shruti Jain, "Can blockchain accelerate Internet of Things (IoT) adoption?", Accessed 31 January 2023, https://www2.deloitte.com/ch/en/pages/innovation/articles/blockchain-accelerate-iot-adoption.html .

[168] Shruti Jain, "Can blockchain accelerate Internet of Things (IoT) adoption?", Accessed 31 January 2023, https://www2.deloitte.com/ch/en/pages/innovation/articles/blockchain-accelerate-iot-adoption.html .

[169] Shruti Jain, "Can blockchain accelerate Internet of Things (IoT) adoption?", Accessed 31 January 2023, https://www2.deloitte.com/ch/en/pages/innovation/articles/blockchain-accelerate-iot-adoption.html .

[170] Mahmoud A. Albreem et al., "Green Internet of Things (GIoT): Applications, Practices, Awareness, and Challenges," *IEEE Access* 9(2021) 38833-38858, https://dx.doi.org/10.1109/ACCESS.2021.3061697 ; Ali Eslami Varjovi, Sharham Babaie, "Green Internet of Things (GIoT): Vision, applications and research challenges," *Sustainable Computing: Informatics and Systems* 28 (2020):100448, https://dx.doi.org/10.1016/j.suscom.2020.100448.

still in its initial stages (the first publications are from 2020) and it definitely seems promising, but there is still not enough literature on it[171].

[171] Mahmoud A. Albreem et al., “Green Internet of Things (GIoT): Applications, Practices, Awareness, and Challenges,” *IEEE Access* 9(2021) 38833-38858, https://dx.doi.org/10.1109/ACCESS.2021.3061697 ; Ali Eslami Varjovi, Sharham Babaie, “Green Internet of Things (GIoT): Vision, applications and research challenges,” *Sustainable Computing: Informatics and Systems* 28 (2020):100448, https://dx.doi.org/10.1016/j.suscom.2020.100448.

Chapter III: State of the Art part II - EU law and the IoEd objects of the smart home

Chapter III: State of the Art part II - EU law and the IoEd objects of the smart home 50
1. Introduction 50
2. Legislative Documents 51
2.1. Data laws and the IoT: an introduction 51
2.2. New and Old Consumer and Contract EU law 61
2.2.1. New technologies and EU Consumer Law 62
2.2.2. Analogue application and progressive adaptation 66
I. The adaptation of the already existent EU Consumer law to the digital revolution 66
II. The New Approach and the New Legislative Framework Acts 69
3. Platform regulation and the IoT 75
3.1. The E-commerce Directive and the proposed Digital Service Act (DSA) 75
3.2. The Digital Markets Act (DMA) 77
4. More technical policy and legislative documents 80
4.1. The EECC, NIS and NIS 2: what they mean for the home IoT 80
5. The long path to AI (and its liability) regulation: consequences for the home IoT objects. 84

1. Introduction

In Chapter II there was a technological analysis of IoT technology, the technological paradigm underpinning the smart home. In this chapter I will focus my attention on how the smart home and IoT technology are actually being indirectly discussed in different EU law and policy fields, by combining a sector specific and a chronological order.

It might be true that the term smart home does not appear frequently as such in policy documents: often, there is reference to AI and new technologies, and quite rarely to the IoT *per se*, but one can imagine that these policy and legislative documents will be applied by analogy depending on the device's level of risk.

This chapter's purpose is to help reconstruct the work of the EU institutions in terms of policy concerning *lato sensu* the development of the IoT for the smart home in a chronological order. I will also combine a thematic order to give a clearer view of the policy and legal development on IoT matters. Therefore, at the beginning of the chapter I will concentrate on what I call "data laws" (2.1). As the GDPR was the first document to be in theory applicable to the IoT, it was important to also group all the other enacted or proposed legislative acts dealing

with data in the same subsection. This approach was also used for EU consumer (2.2), platform regulation (3) and cybersecurity (4) proposed and enacted legislative acts. The last section of the chapter instead tackles how the liability theme of new technologies was dealt with by the EU institutions and which consequences there might be for IoT home objects (5). At the end of this chapter, there will be a brief timeline that sums up the results of the EU Digital Strategy, that was helpful in selecting the material which will be commented on in the following sub-sections and sub-paragraphs.

2. Legislative documents

The grouping and schematisation of all the legislative documents present in this subsection have been obtained by intersecting two criteria. The first is a thematic one: the different enacted and proposed legal acts are divided according to their theme (their relationship to data and consumer law). The second criterion instead is a chronological one: within each of the thematic blocks, I will re-arrange the several legal acts in chronological order.

2.1. Data laws and the IoT: an introduction

It has already been established from the technical description of the IoT and how it works in a smart home that data is important: without it, or, more correctly without a considerable quantity of it, the algorithms that are currently mostly in the cloud (and not inside the device) would not be able to analyse the patterns of use that people in the home create. Hence, they would not be able to infer their habits and help in anticipating their needs.

Following a chronological order, the first EU legislative document that can be applied to the IoT in smart homes is the General Data Protection Regulation (GDPR)[172]. Approved in 2016 but effective from 2018, the GDPR was the first effort to regulate pervasive new technologies. It follows a horizontal approach, meaning that it is applied insofar a more specific document or legislative act is applicable. It substitutes the previous Data Protection Directive (DPD)[173]. In this

[172] "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) *OJ L 119*, 4.5.2016, p. 1–88", EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679&qid=1661353452590.

[173] As far as definitions and principles are concerned, the two legislative acts are quite similar, but they also differ in significant ways. According to the sources of EU law, the DPD is mandatory only in the effects, but MS had a certain leeway to transpose the legislation into their own legal system. The GDPR is instead a regulation and this means that, unless prescribed otherwise, it is mandatory as far as the means outlined and the results expected by the document itself. This also witnesses a change in society towards personal data and technology in general: the fact that this act has a higher hierarchical status than before means that these issues are taken more seriously by EU citizens and their EU representative. Not to mention that the GDPR is the first attempt to adopt a technology-neutral approach that tries to find a balance by stating that there are principles (which is the most similar part to the former DPD, together with the subjects of the data processing activities) to the fundamental right of data protection and also a risk-

subsection there will not be an explanation of all the GDPR rules, but I will try to highlight the main points of friction between the IoT technology for the smart home as it is thought of and designed nowadays, at least most of the time, and the GDPR itself.

The main problem both for IoT manufacturers and for consumer IoT is how to tell apart personal data from non-personal data. Already in the early 2010s, Ohm[174] argued that what is personal or not depends on context, which in the home IoT object context is considered to be twofold. On the one hand, there is the relationship between the user and the object. On the other hand, there is the object's technological advancement, which also influences the way of protecting data. Generally, the CJEU has always had a rather wide conception of personal data[175], and the former Article 29 working party, later substituted by the EDPB, shared this view. This wide interpretation rationale was used to better protect the data subject's fundamental right to data protection. The almost open-ended definition of personal data was used again in the GDPR regulation. Article 4(1) GDPR defines that data from which a person can be identified or is identifiable as personal. The fact that identifiable is mentioned means that data is considered personal if it is possible to single out an individual, even if, for instance, their identity is not manifestly recognisable. If, on the one hand, this approach is laudable, as it protects people from non-apparent forms of discrimination[176], on the other hand it risks GDPR being applied to more and more kinds of data, thus increasing the compliance duties and obligations that must be performed by controllers (who bear the outright majority of them) and not all controllers can afford that. Therefore, it must be avoided that data protection becomes "the law of everything", as Purtova effectively states[177].

based approach. For a better level of governance, in fact, not only are national Data Protection Authorities (DPAs) coordinated by a proper EU body, the EDPB, but also enterprises can be compliant by also periodically reviewing the risks of violation of data protection rules through Data Protection Impact Assessments (DPIA). See also "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data *OJ L 281*, 23.11.1995, p. 31–50," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046.

[174] Paul Ohm, "Broken promises of privacy: Responding to the surprising failure of anonymization," *UCLA Law Review* 57,6 (2010):1701-1777.

[175] Also Internet Protocol (IP) addresses, even the dynamic ones, were recognised as personal data in the *Breyer* case. "Patrick Breyer v Bundesrepublik Deutschland, Case C-582/14," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62014CJ0582.

[176] In the US, algorithm-based data processing techniques have made racial discrimination explicit in activities such as credit pricing and mortgages, to the detriment of African Americans. See Talia B. Gillis, "The Input Fallacy," *Minnesota Law Review*, forthcoming 2022, Accessed 31 January 2023 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3571266. However, synergies between academic pinpointing cases of algorithmic discriminations and economic operators such as large platforms employing them can happen. For example, on the basis of the work on the Conditional Demographic Disparity Sandra Wachter, Brent Mittelstadt and Chris Russell, the "sexist" hiring algorithms employed by Amazon could be changed and become fairer through the new bias toolkit "Amazon Sage Maker Clarify". Oxford Internet Institute, "Press Release - AI modelling tool developed by Oxford Academics incorporated into anti-bias software," Accessed 31 January 2023, https://www.oii.ox.ac.uk/news-events/news/ai-modelling-tool-developed-by-oxford-academics-incorporated-into-amazon-anti-bias-software-2/.

[177] Nadezhda Purtova, "The law of everything. Broad concept of personal data and future of EU data protection law," *Law Innovation and Technology* 10,1 (2018):40-81, https://dx.doi.org/10.1080/17579961.2018.1452176.

Generally, when data is personal, the controller, meaning the subject that is in charge of determining the means and scope of the processing[178], has to be aware that at least one of the conditions listed in Article 6 GDPR is present. One of the main legal bases used when installing an app that allows a smart object to function is consent, which should be freely given, made after an informed choice and for one or more purposes that have been illustrated in the data protection/privacy policy/ terms and conditions according to Article 7 GDPR. However, since the beginning of 2000s it has become known that data subjects confirm that they give consent to data controllers and processors through "privacy self-management" systems, and seldom have any idea of all the implications of their choice[179]. It goes without saying that whenever consent is not freely given and, especially in an interconnected environment, whenever several objects are working all at once, it should also be easy to withdraw this consent, or to consider the data processing activities performed as unlawful[180].

Furthermore, IoT objects for the home are already using not only data that can identify or make identifiable the user or the people in the home (even the ones that come from different households) but also special categories of personal data. Among the categories of data that cannot be processed, article 9(1) GDPR also lists genetic, biometric and health-related data. An increasing number of devices now "want" us to use our fingerprint, our heartbeat, our face image or our voice[181] to perform. These kinds of data, however, are respectively biometric data, health-related data, and genetic data within the meanings of Article 4(1),(13), (14),(15) GDPR. Article 9(2) GDPR provides some basis for processing and, generally, private actors such as the producers of home IoT generally use a specific kind of consent, set out in Article 9(2)(a) GDPR in order to carry out the process lawfully. Nevertheless, the problems concerning the validity of consent are the same in this case. They are made even more serious as health, and everything related to the "datafication" or "commodification" of the human body is always addressed from an ethical and not just legal point of view.

It is true that not all data processed in the home is personal, a large portion are simple log-in/out inputs that are stored either *in situ* or in the cloud. Until the Data Act proposal[182] comes into force, there is currently no appropriate way to take advantage of this kind of non-personal data, especially for EU

[178] Article 4.7 and 24, 26, and 27 GDPR
[179] Daniel Solove, "Introduction: Privacy Self-Management and the Consent Dilemma," *Harvard Law Review* 126,7 (2013) 1881. To understand how difficult it is, especially in the US, to make businesses obtain high quality consent see also Chris Jay Hoofingale, "Designing for Consent," *Journal of European Consumer and Market Law* 4(2018):162-171.
[180] Article 7(4) GDPR and Fundamental Rights Agency of the EU and the Council of Europe, *Handbook of European Data Protection Law* (Luxembourg, Fundamental Rights Agency of the EU and the Council of Europe: 2018), 112, https://dx.doi.org/10.2811/343461.
[181] Which is considered as personal and unique data according to CNIL, see Chapter II.
[182] "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (Data Act)
COM/2022/68 final" EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN.

manufacturers[183]. The Free Flow of Data Initiative regulation[184] (ironically also the only EU legislative act to name the IoT for a long time, without defining it) has tried to give examples on how to tell apart personal data from non-personal data, but not living up to its objective to create an environment of data-sharing among manufacturers in order to make the IoT technology stronger in the EU[185].

With its Data Governance Act (DGA) regulation proposal, now regulation[186], the Commission in part wants to achieve what the FFDI has failed to do so far and also promote the creation of new sharing intermediaries along with new values and concepts including the one of data user[187] and data altruism[188]. Despite the fact that the EU Parliament and the Council seem to have reached an agreement on the proposal[189], it has still not been completely proven that the DGA will be more effective than its predecessor the FFDI and especially the Open Data Directive with which it is in a relationship of complementarity [190].

In a similar way to the difference between personal and non-personal data, it is almost impossible to avoid describing any process involving data in the home except with the label of data processing of Article 4.2(4) GDPR. Processing in fact relates to all automated (wholly or partly) or non-automated means to work with personal data and it involves a wide range of activities, from storage to structuring. There are some insurances against fully automated processing in Article 22 GDPR. The data subject/user can opt out from a processing technique that does not involve a human at all. Nevertheless, there are three important exceptions. Article 22 (2) GDPR states that the first paragraph (the opting out option) is not permitted whenever the automated processing is "(*a) essential to perform or fulfil the contract, (b) whenever the EU or Member state law expressly authorises this kind of processing, and (c) also when the data subject has expressly given their consent to the processing*[191]**"**. It is not that difficult to imagine that a data subject both fulfils the conditions for the first and third exception by effectively purchasing an interconnected good, such as a domestic IoT object

[183] Josef Drexl, "Designing Competitive Markets for Industrial Data - Between Propertisation and Access," *JIPITEC* 4 (2017) 261- 267.
[184] "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," Eurlex, Accessed 13 August 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1807.
[185] Maria Lillà Montagnani," La libera circolazione dei dati al bivio. Tra tutela dei dati personali e promozione dell'intelligenza artificiale europea," *Mercato Concorrenza Regole* 2 (2019): 310-305, https:/dx./doi.org/10.1434/95581.
[186] "Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance) PE/85/2021/REV/1 *OJ L 152, 3.6.2022, p. 1–44*," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868. Hereinafter, DGA.
[187] Article 2(6) DGA "'data user' means a natural or legal person who has lawful access to certain personal or non-personal data and is authorised to use that data for commercial or non-commercial purposes;"
[188] Article 2(10) DGA "'data altruism' means the consent by data subjects to process personal data pertaining to them, or permissions of other data holders to allow the use of their non-personal data without seeking a reward, for purposes of general interest, such as scientific research purposes or improving public services".
[189] Luca Bertuzzi "Data governance: new EU law for data-sharing adopted," *Euractiv*, December 01, 2021, https://www.euractiv.com/section/digital/news/data-governance-new-eu-law-for-data-sharing-adopted/.
[190] See Article 1(2)(a),(b) DGA, Julie Baloup et al., *White Paper on the Data Governance Act*, (Leuven: CiTiP Working Paper Series, 2021), https://dx.doi.org/10.2139/ssrn.3872703.
[191] Article 22(2)(a),(b),(c) GDPR.

(e.g., cleaning robot) and then by accepting the "terms and conditions" and "privacy policies" on the smartphone application of the same object.

It is true that the GDPR also mandates the controller to have a transparent and clear communication with the data subject[192]. Especially as far as consent is concerned, Article 7(2) GDPR explicitly states that whenever the indications concerning data protection are in writing, they should be intelligible and written in clear and plain language[193]. There is still not enough evidence to fact-check whether the situation has improved under this aspect since the introduction of the GDPR. What should be instead mentioned is that researchers and national Data Protection Authorities (DPAs) have taken on a pro-active role in indicating ways to use techniques of Legal Design, legal ontologies and visualisations to create privacy friendly icons[194], a task that the GDPR itself formally attributes to the Commission in accordance with Articles 12(8) and 93(2) GDPR. These initiatives are particularly welcomed as even pre-GDPR literature certified that behavioural biases in consumer-data subjects lead them to trade data and have better quality services[195].

In the GDPR, despite there already being several provisions that could be applied to the IoT, including domestic ones, there is one of the few mentions involving the home environment in Article 2(2)(c). This provision is known as "the household exemption". This means that any data processing activities occurring in the house are exempted from application of the GDPR. The household exemption was already present in the previous DPD and it not only concerns the application field of the whole GDPR but also the hierarchy, in terms of accountability (Articles 5(2) and 24 GDPR), responsibility (Articles 24, 28 GDPR) and liability (Article 82) of the different subjects involved in the data processing. This hierarchy will be briefly described in the following paragraph.

While the data subject is the natural person to whom the personal data is attributed/attributable, the controller and processors are more directly involved in the processing phase. On the one hand the controller determines the means and purposes of the processing[196]; on the other hand, the practical and concrete

[192] Article 12 GDPR.
[193] Article 7(2) and 12(1)(2) of the GDPR.
[194] As far as privacy icons contests, the Italian DPA (Garante per la Protezione dei Dati Personali) launched a competition for creating more understandable privacy icons in 2021 awarding prizes to the three winners and one special mention. Garante Privacy, "'Transparent Information': winners of the contest launched by Italian SA announced," Accessed 31 January 2023, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9727383#english. In academia and research environments, data visualisation and legal design initiatives also need to be mentioned. This issue has been investigated both from a more theoretical angle but also a practical one. See Arianna Rossi and Monica Palmirani, "DAPIS: An ontology-based data protection icon set," in *Frontiers in the Artificial Intelligence Applications*, Ginevra Peruginelli and Sebastiano Faro (Amsterdam: IoS press, 2019), 188-193; and Zohar Efroni et al., "Privacy icons: A risk-based approach to visualisation of data processing," *European Data Protection Law Review* 5,3 (2019): 357-366, https://dx.doi.org/10.21552/edpl/2019/3/9.
[195] This is usually done by relying on heuristics, which allows to use simplified reasoning that by privileging one aspect of a given set of information, which could also result on misconceptions. Zohar Efroni et al., "Privacy icons: A risk-based approach to visualisation of data processing," *European Data Protection Law Review* 5,3 (2019): 356, https://dx.doi.org/10.21552/edpl/2019/3/9.
[196] Articles 4(7) and 24 of GDPR.

actions of processing as described in Article 4(2) GDPR are often carried out by the processor[197], which must be tied to the controller by an agreement in writing. Despite this apparently simple distinction, both the Article 29 Working Party, and the EDPB have insisted on the fact that both controller and processor concepts are *functional* ones[198]. It means that depending on the degree of autonomy and on the functions actually exercised, even a formerly qualified processor can be considered as a controller (for instance when it acts beyond the instructions given, or with gross negligence). Hence, it could be held liable in case of data breaches and infractions of data protection. To be complete, this hierarchy must also include a mention of third parties and data recipients in Article 4(9),(10) GDPR. Mainly, the difference between these last two categories is the relationship that they have with controllers and processors: third parties are authorised contractually by either the controller or the processor to process data subjects' personal data, while the recipient category instead is larger. There is no relationship between controller/processors and recipients and can be summarised as the subject (natural/legal person, public authority or agency) to whom data is disclosed[199].

The fact that controllers and processors must be judged from facts rather than from contractual formalities can appear more protective of data subjects, but it could be a two-edged sword. If the threshold level concerning control over data is gradually lowered, then the application of the household exemption is rarer as new subjects, including data subjects, could be considered to have a meaningful control over other people's personal data. Consequently, they could be considered joint controllers without being aware of it[200]. This was the approach

[197] The full extent of the duties and responsibilities will be dealt with in Chapters V and VI. For the moment suffice to say that both the controller and the processor can be natural or legal persons and also public authorities, agencies and other bodies, as stated in Article 4(7),(8) GDPR.
[198] EDPB, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR - Version 2.0* (2021), 9, Accessed 04 February 2022, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en; Article 29 Working party, *Opinion 1/2010 on the concepts of "controller" and "processor"* (2010), 11, Accessed 31 January 2023 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf. Brendan Van Alsenoy, *Data Protection Law in the EU: Rules Responsibilities and Liability*, (Antwerp, Cambridge, Portland: Intersentia, 2019), 63.
[199] Brendan Van Alsenoy, *Data Protection Law in the EU: Rules Responsibilities and Liability*, (Antwerp, Cambridge, Portland: Intersentia, 2019), 63.
[200] According to Article 26 GDPR, it is possible to have joint controllership but there must be a written agreement between the joint controllers. This is essential in order to establish the controllers' respective liabilities in the event of a data breach.

adopted by the CJEU[201] and the 29 Working Party[202] before the application of the GDPR and by the EDPB[203] after the GDPR enactment.

Moreover, the introduction of the principle of accountability of the controller in Article 5(2) GDPR[204] is founded on the assumption that by making the largest number of subjects accountable and responsible for compliance, data subjects would be more protected[205]. This is disputable: especially in automated environments, the relationships between controller, processors, third parties and recipients extend way beyond the perimeter of the home and are becoming increasingly complex[206]. As an example, we have to consider the producers of objects, which are also data controllers most of the time, but also processors (mainly cloud services providers which automatise the processing phase), third parties (for instance "partners" or "advertisers" on an application), data subjects (who may or may not be living in the house) whose data are processed and recipients (e.g., another physical person is able to observe the performance parameters of a another data subject's smart thermostat due to a bug in the information system).

The number of subjects involved must be multiplied by the number of smart objects in the house. In addition to that, the growing level of interoperability between objects will create situations of more or less known controllership even among different enterprises which build IoT objects for the home. Among the home IoT actually sold, users have raised issues concerning the voice assistants' capacity to activate autonomously and sometimes when other people who do not

[201] The lowering of the bar of controllership intensity is found in several judgments. For instance, in *Wirtschaftsakademie,* the owner of a Facebook page who was using Facebook analytics to monitor the success of the page was considered a joint controller with Facebook, paras 35-44, in "Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH, Case C-210/16." EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62016CJ0210. A similar situation occurred in *Fashion ID*: an operator of a website which installed social plug-ins that made it possible for the provider of the plug-ins to process those data. Both the operator and the provider were considered joint-controllers, paras 75-80. See "Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV., Case C-40/17," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62017CJ0040. In *Ryneš*, the household exemption was instead called into question to exclude Mr Ryneš' recording from his CCTV system being used as evidence against two people who had allegedly broke into his home. The CJEU did not consider that this processing activity fell within the household exemption (paras 28-35), "František Ryneš v Úřad pro ochranu osobních údajů, Case C-212-13," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62013CJ0212.

[202] Apart from the Opinion 1/2010 on the notion of controller and processor, the Article 29 Working Party established that if the user did not manage its privacy settings on social media, leaving its information potentially available to everyone, then the household exemption was not applicable. Article 29 Working party, *Opinion 5/2009 on online social networking*, 12 June (2009): 5-6, Accessed 31 January 2023, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf

[203] EDPB, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR - Version 2.0* (2021), 9, Accessed 31 January 2023, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en

[204] This means that the controller not only has to demonstrate the application of data protection principle but also how the system is made and reacts in order to reduce the risks. EDPB, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR - Version 2.0* (2021): 8-9.

[205] Michelle Finck, "Cobwebs of control: the two imaginations of the data controller in EU law" *International Data Privacy Law* 11,4 (2021) 333, https://dx.doi.org/10.1093/idpl/ipab017.

[206] Michelle Finck, "Cobwebs of control: the two imaginations of the data controller in EU law" *International Data Privacy Law* 11,4 (2021) 333, https://dx.doi.org/10.1093/idpl/ipab017.

belong in the house are present[207]. Where does this leave the IoT owner whose IoT object activates autonomously and processes another data subject's /third party's personal data without their consent? According to the judgements cited, there is a high chance that they could be considered a joint controller because they could have prevented the automatic activation of the voice assistant from occurring. The increasing complexity given by interconnected environments and the strict interpretation of the household exemption make it clear that the possibility for a data subject to become a joint controller despite themselves clashes with the GDPR's main objective to protect a data subject's fundamental rights and freedoms. This would go against Article 26 GDPR which establishes that joint controllers should divide their respective duties and obligations as far as data processing and GDPR compliance are concerned between themselves. In this sense the issues raised by scholars concern the vanishing of the application of the household exemption[208] and the outdated notion of consent[209] and, also, the *de facto* difficult allocation of responsibility and liability between data controllers and processors[210].

Finally, the last point of friction between home IoT objects and the GDPR is Article 82 GDPR on data controller(s) and processor(s) liability. In particular, no one knows how Article 82 GDPR would be applied in a connected environment such as the future smart home. The article establishes the principle of full compensation of both material and immaterial damage. As will be explained further in Chapter V[211], judges in MS are currently discussing the application of this article. A literal interpretation would mean that each violation (even one that is not directly harmful) for the data subject should always be compensated. As will be explained in Chapter V, this view is not shared by some courts which always ask for proof of the harm suffered[212]. Moreover, Article 82(4) and (5) GDPR establish that whenever there is more than one controller and processor that are involved in a GDPR liability case, they are held liable for the entire damage. The data subject could ask to be compensated by each of them (generally the more solvent of the group) and later the data controller or processor who has paid should be granted recovery action towards the remaining co-debtors by the MS. However, it all depends on MS procedural laws how to also quantify the responsibility of each of the co-debtors involved, a task that would

[207] Sam Shead, "Amazon Echo and Google Home owners spied on by apps," *BBC News Tech*, October 21, 2019, https://www.bbc.com/news/technology-50124713.
[208] Silvia De Conca, "Between a rock and a hard place: owners of smart speakers and joint control," *SCRIPT-ed* 17,2 (2020): 252-254, https://dx.doi.org/10.2966/scrip.170220.238; Jiahong Chen, Lilian Edwards, Lachlan Urquart and Derek McAuley," Who Is Responsible for Data Processing in Smart Homes? Reconsidering Joint Controllership and the Household Exemption," *International Data Privacy Law* 10,4(2020): 279-293, https://academic.oup.com/idpl/article/10/4/279/5900395 .
[209] Michelle Finck, "Cobwebs of control: the two imaginations of the data controller in EU law" *International Data Privacy Law* 11,4 (2021) 333, https://dx.doi.org/10.1093/idpl/ipab017; Jiahong Chen et al., "Who Is Responsible for Data Processing in Smart Homes? Reconsidering Joint Controllership and the Household Exemption" *International Data Privacy Law* 10,4 (2020): 284-286, https://dx.doi.org/10.1093/idpl/ipaa011.
[210] Brendan Van Alsenoy, *Data Protection Law in the EU: Rules Responsibilities and Liability* (Antwerp, Cambridge, Portland: Intersentia, 2019), 83-116.
[211] See Chapter V, Section 3, Future Article 9 PLD.
[212] That is the case of the Italian Court of Cassation. See Ordinanza Cassazione n.16402/2021, Accessed 31 January 2023, https://i2.res.24o.it/pdf2010/Editrice/ILSOLE24ORE/QUOTIDIANI_VERTICALI/Online/_Oggetti_Embedded/Documenti/2021/06/11/16402.pdf

not be a simple one for a connected environment. Furthermore, each of these specific procedural laws will differ in each and every MS, hence there would be a problem of actual and fair enforcement of this provision.

With regard to the content that the data subject might create/help to create through the use of personal data, a further layer of protection will be added as the content will be subjected to the E-Privacy directive[213], whose renewal proposal has been reported since 2017[214]. The last presidency to be active in this sense was the Portuguese one, which stated that the E-Privacy directive should be a *lex specialis*[215] compared to the GDPR (even though coordinated with the latter). This can be explained by the fact that protection is given to personal data and to the information it carries, thus enforcing Article 7 of the Charter of fundamental rights. Moreover, because the E-Privacy directive covers metadata (which literally means data about data), it could be applicable to domestic IoT objects as they need to share their location data with their producer, which is important as location data could also be considered to be personal data as it indirectly reveals personal information about a person. From the metadata obtained from a cleaning robot, it is possible to understand the wealth of a person: for instance one can infer that from the floor surface area that the robot needs to clean or the type of neighbourhood in which the home is located. Or, thanks to a smart fridge, the producer can know whether a person prefers to eat certain kinds of food (for instance vegetables or fruit) and can infer that it is because of a religion or a philosophical reason, all of which is inferred personal data. According to the most recent draft of the proposal, the sharing of metadata is allowed (with the consent of the data subject) and might be subjected to analysis and predictions which could infer personal information about the person. For instance, the "likes" a user puts on social media (a like is not personal data per se) might be transmitted (because of the consent given when subscribing to the service) to third parties from which personal data can be inferred, such as political and religious beliefs[216]. That is why in the latest draft. IoT objects should be included and considered as interpersonal communication, hence protected, whenever the IoT is not in a closed circuit[217].

The latest addition in terms of data laws that will be applied to the IoT is the proposal for a regulation on harmonised rules regarding fair access to and

[213] "Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)," Eurlex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058 .
[214] "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) COM/2017/010 final - 2017/03 (COD)," Eurlex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010.
[215] Article 95 GDPR states that the GDPR itself will not impose further burdens on the E-Privacy directive. The text of the latest draft of the Council of the EU for the E-Privacy directive is accessible. "Confidentiality of electronic communications: Council agrees its position on ePrivacy rules," European Council, Council of the European Union, Accessed 31 January 2023, https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf.
[216] Recital 2 of the Commission's Proposal for the E-Privacy Directive.
[217] 12 of the Council Proposal (Portuguese presidency 1st semester 2021).

use of data, the so-called Data Act (DA), which the European Commission presented in February 2022. This proposed regulation builds on the legacy previously explained of the Free Flow of Data Regulation (FFDR, which is expected to be repealed during the course of 2022-2023), with the objective of complementing the DGA, the FFDR, and the newly approved Digital Markets Act (DMA, more on that *infra*).

There are several objectives for the Data Act, as explained in the memorandum accompanying the proposal: "

- *Facilitate access to and the use of data by consumers and businesses, while preserving incentives to invest in ways of generating value through data […]*
- *Provide for the use by public sector bodies and Union institutions, agencies or bodies of data held by enterprises in certain situations where there is an exceptional data need*
- *Facilitate switching between cloud and edge services*
- *Put in place safeguards against unlawful data transfer without notification by cloud service providers*
- *Provide for the development of interoperability standards for data to be reused between sectors*
- *Consistency with existing policy provisions in the policy area*[218]"

This proposal, if approved, is going to radically change the regulation of big data economics so far, as it grants a right of access to data, both personal and non-personal, and to both legal and natural persons, under certain conditions. This right can be used towards data-holders, meaning physical or legal persons that collected, or have availability and access to large quantities of data, such as an IoT producer, and that has the obligation under the Data Act to make them available[219].

Although this proposal will be better explained in Chapter IV and V due to the evident connections with product liability issues for domestic IoT objects, I will now provide an explanation of the DA' s connection to both IoT objects (including ones for the smart home) and to the GDPR. Interestingly, this document contains an extended definition of an IoT object although it is simply called "product". It differs from the cybersecurity definitions that will be explained infra at section 3 of this Chapter, as in those cases the IoT is considered as a networked system, while in the DA an IoT may just coincide with a consumer product. The fact that it is applicable to the IoT can be inferred from Article 2 (2) of the Data Act: "'*product' means a tangible, movable item, including where incorporated in an immovable item, that obtains, generates or collects, data concerning its use or environment, and that is able to communicate data via a publicly available electronic communications service and whose primary function is not the storing and processing of data*"[220]. Moreover, the term IoT is referenced also in recital 14 with a slightly different formulation. This proposal might be the most "horizontal" in terms of applications, as it is likely that it will apply indiscriminately to all IoT

[218] "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (Data Act) COM/2022/68 final," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN. Hereinafter DA.
[219] Article 2(6) DA.
[220] Article 2(2) DA.

objects on the basis of a "general to special" rationale, without any distinction on the kinds of data that are processed, provided there is the consent of the data subject whose data are requested by someone else (be it a company or another physical person).

The EU Commission maybe is convinced that the Data Act discipline is not in contrast with the GDPR, but, if anything, it reinforces some of its Articles such as Article 15 GDPR on transparency and access (the generalised right of access being one of the main legal innovations of the last years) and Article 20 GDPR on interoperability as, especially for this last aspect, the Data Act has devoted an entire Chapter to it (Chapter VI DA). On the contrary, in their joint opinion of May 2022, the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) express concern about the breadth of possible application of the DA, especially as far as health data and other kinds of personal data are concerned. In principle, "[…] *this proposal is applicable to all kinds of IoT and Internet of Bodies (IoB) devices*[221]. The EDPB and EDPS believe that it should be made explicit that the GDPR takes precedence over the Data Act in the event of discrepancies[222]. Moreover, they suggest some key definitions, such as the one for product, be more defined as in the actual draft it would overlap with the current definition of terminal equipment in the E-privacy directive[223]. The definition of data should also make reference to personal or non-personal data[224]. Finally, the Opinion highlights how the Data Act is silent and does not mention the data subject in the vent that they disagree with the terms and conditions of making their data available, when "*personal data are made available to third parties upon a request of users who are not the data subjects,*" as "[…] *the latter would be completely excluded from the participation to dispute settlement proceedings concerning the sharing of their personal data between the data holder and the data recipient*"[225]. This would lead to the paradoxical result of the DA lowering the level of protection guaranteed by the GDPR. It is yet to be seen whether the Commission will actually follow these guidelines.

2.2. New and old EU consumer and contract law

European consumer law and the new policies and initiatives that have been promoted in recent years never explicitly mentioned either smart homes or the IoT. Energy law took on this role to a greater extent initially[226]. The New Consumer Agenda, however, tries to strike a balance between the digital innovation that has invested consumer law and environmental concerns, as already explained in Chapter II. As far as the relationship of EU consumer law

[221] §13 of the Opinion. EDPB-EDPS, *Joint Opinion 2 / 2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act),* Adopted on 4 May 2022, Accessed 31 January 2023, https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-22022-proposal-european_en . Hereinafter EDPB-EDPS, Opinion 2/2022.
[222] EDPB-EDPS, Opinion 2/2022, 2.
[223] §§40, EDPB-EDPS, Opinion 2/2022.
[224] §38 EDPB-EDPS, Opinion 2/2022.
[225] §64 EDPB-EDPS, Opinion 2/2022.
[226] See Chapter II.

with the home IoT technology is concerned, legislative acts and documents respond to two different kinds of inputs. Existing legislative acts concerning consumers and technology can be divided into two groups: *i)* the ones that take into account new technologies from their drafting *ii)* the ones with texts drafted before or at the very beginning of the advent of digital technologies, that are interpreted or updated in such a way that they can be applied to existing technology, including the IoT, until a formal re-cast or amendment by the EU Parliament and Council.

2.2.1. New technologies and EU consumer law

With regard to the first group of legislative acts, the two directives on certain aspects concerning contracts for the the sale of goods no.771/19 (which include also contracts for the sale of goods that have interconnected software, hence in this thesis it will be abbreviated as SDG, as in sale of digital goods)[227], and the directive no. 770/19 on certain aspects concerning contracts for the supply of digital content and digital services (DCDS)[228] are applicable to IoT objects, especially the ones for the home. The directives are complementary in content, and they are both full harmonization instruments[229] . The main innovation from a legal point of view is to consider the exchange of data as a form of payment for the consumer[230] but also that the object or service is the starting point for creating these new contracts and not the typology of contract[231].

These directives and their evolution, from proposals to existing legislative acts, have been commented and described in depth[232], therefore I would like to focus solely on a few points of interest in relation to domestic IoT technology.

The first one is that technology vocabulary is appearing more and more frequently to explain EU consumer law legal concepts. For instance, in both directives, conformity, which is a relative term[233], must be assessed and evaluated through a list of subjective and objective criteria. In the SDG, Article 6 concerns the subjective requirements for conformity. In letter *a)* of the same

[227] "Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC (Text with EEA relevance.) PE/27/2019/REV/1 *OJ L 136, 22.5.2019,* p. 28–50" EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32019L0771.

[228] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services (Text with EEA relevance.) PE/26/2019/REV/1 *OJ L 136, 22.5.2019*, p. 1–27", EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L0770.

[229] Jorge Morais Carvalho, "Sale of Goods and Supply of Digital Content and Digital Services – Overview of Directives 2019/770 and 2019/771" (2019) 5, 194.

[230] Karin Sein and Gerald Spindler, "The new Directive on Contracts for Supply of Digital Content and Digital Services – Conformity Criteria, Remedies and Modifications – Part 1*" European Review of Contract Law* 15(2019): 365.

[231] Karin Sein, "What Rules Should Apply to Smart Consumer Goods ? Goods with Embedded Digital Content in the Borderland Between the Digital Content Directive and "Normal " Contract Law" *JIPITEC* 8(2017):96.

[232] In addition to the previously cited sources on the matter see also Alberto De Franceschi, *La Vendita dei Beni con Elementi Digitali* (Edizioni Scientifiche Italiane 2019).

[233] Recital 25 SDG.

article, some technical characteristics, such as functionality, compatibility, and interoperability[234] are key to meet the conformity obligation. This attention to technical language is also present in the following article which describes the objective criteria. In fact, in Article 7 SDG, there is an explicit mention of "technical standards" or "industry specific codes of conduct" as references to evaluate the fitness of the object for the purpose[235]. The same wording can be found respectively in Article 7(a) and Article 8(a) DSDC.

The "twin" directives mirror and complement each other in their own structure even further. This becomes evident when reading the definition of digital content or service and digital goods, which are key in order to know which of the directives to apply. In particular, the definition of digital goods is thought of by having some consumer IoT objects as references as shown in the SDG recitals[236]. In Article 2(5)(b) SDG digital goods are considered as *"…any tangible movable items that incorporate or are inter-connected with digital content or a digital service in such a way that the absence of that digital content or digital service would prevent the goods from performing their functions ('goods with digital elements')"*. Instead, the definitions of digital content covers "*data that are produced and supplied in the digital form*"[237] and digital service as both *"a) a service that allows the consumer to create, process, store or access data in digital form; or (b) a service that allows the sharing of or any other interaction with data in digital form uploaded or created by the consumer or other users of that service"*[238]. Despite the apparent clarity of both definitions, in real life it is not often that easy to assess whether an application, which could provide a service and/or content, and that could either be installed or pre-installed on a device, should fall within the application of either the SDG or DCDS.

According to the recitals of both directives[239], the contract of sale connecting the seller of the goods with a digital element and the consumer is key: if the supply of the inter-connected digital content and digital service forms part of the sales contract the SDG should apply[240]. There are also some examples in the recitals. For instance, if *"…a smart TV were advertised as including a particular video application, that video application would be considered to be part of the sales contract."*[241]. There were other rules discussed to address this scenario, such as the rule concerning linked contracts. Nevertheless, in the end

[234] This lexicon is interesting to analyse as it testifies how technical jargon is slowly making its way into legal text, the first example being the GDPR with the introduction of profiling, automated decision making and data portability. Moreover, in the SDG and DSDC in Article 2 (8),(9),(10) the concepts of compatibility, functionality, interoperability are explained in detail.
[235] Article 7 (a) SDG.
[236] In particular, in the SDG explicitly mentions "smart watch" in recital 14, "smart tv" in recital 15 and "smart phone" in recital 16.
[237] Article 2(6) SDG and Article 2(1) DCDS.
[238] Articles 2(7)(a),(b) SDG and 2(2)(a),(b)DCDS.
[239] More specifically recitals 15-16 SDG and 21-22 DCDS.
[240] Karin Sein, "What Rules Should Apply to Smart Consumer Goods ? Goods with Embedded Digital Content in the Borderland Between the Digital Content Directive and "Normal " Contract Law" *JIPITEC* 8(2017):96; Karin Sein and Gerard Spindler, "The new Directive on Contracts for the Supply of Digital Content and Services- Scope of Application and Trader's Obligation to supply-Part 1," *European Review of Contract Law* 15,3 (2019):270-271, https://dx.doi.org/10.1515/ercl-2019-0016.
[241] Recital 21 DCDS.

the simplest rule was chosen, which was suggested by the Council when discussing the proposal[242]. This rule is likely to make the sellers overburdened as far as liability is concerned, especially if we consider that whenever there is the doubt about whether the service is essential to the functioning of the goods, it will be presumed that the lack of conformity is covered by the sales contract[243], and therefore paid by the seller.

This is not always fair if we think that the leading digital services traders or providers can have a powerful influence on both producers and sellers. In fact, the more it gives access to well-known digital services, the more the item will appeal to the public. Examples of applications that have become *de facto* indispensable are internet providers, platforms and social networks. Hence, contractual relationships can be imbalanced, and producers and sellers might be forced to accept digital traders' conditions in terms of interoperability and compatibility with the services offered. As a consequence, they would not be entitled to have a form of recovery action as the lack of conformity "has become" their own, something they have agreed to. This is something that is already happening: the Preliminary report of the Sector Inquiry on Consumer IoT (now known as Staff Working Document- Report on the Consumer IoT) demonstrated that the major voice assistant providers were already laying down conditions on how to make other producers' IoT devices interoperable with their software [244] .

The third interesting point to analyse regarding the two directives is how to evaluate whether the seller (SDG) or trader (in the DCDS) are compliant with their obligation of conformity and the structure of remedies. The DCDS adds the obligation to supply the digital content or service in Article 5, which will also be assessed with subjective and objective criteria. Moreover, the obligation includes the duty of correct integration of the digital content or digital service[245]. It is evident that the articles concerning compliance in the SDG and the DCDS are Articles 6,7,8.

Among the objective criteria to evaluate conformity of the goods, content or service, it is particularly interesting that the seller/trader informs the consumer and supplies them with updates, including security ones[246]. If the consumer fails to install them within a reasonable time, the fault should not lie with the seller/trader but with the consumer[247]. This issue is particularly sensitive with home connected goods, as device providers do not often build their devices to last a long time. This creates the "lock-in" effect through which sellers and traders can maintain consumers by *de facto* obliging them to update their system regularly. In the worst cases, programmed obsolescence obliges consumers to

[242] Karin Sein and Gerard Spindler, "The new Directive on Contracts for the Supply of Digital Content and Services- Scope of Application and Trader's Obligation to supply-Part 1," *European Review of Contract Law* 15,3 (2019):270-271, https://dx.doi.org/10.1515/ercl-2019-0016.
[243] Article 3(3) SDG.
[244] Commission Staff Working Document, "Preliminary Report- Sector Inquiry Into Consumer Internet of Things" Brussels, 9.6.2021, SWD(2021) 144 Final.
[245] Article 9 DSDC.
[246] Article 8(2) DCDS and Article 7(3) SDG.
[247] Article 8(3)DCDS and Article 7(4) SDG.

buy another similar device after a while. The choice to buy a newer model of the same object is dictated by the fact that, through using the device, the consumer may have bought other devices or applications which were interoperable with that brand of object. If they do not want to lose this "primordial" home networked environment, they will still buy a device or service by the same trader or seller [248]. The focus here should be on the difference as to when the update is simply an update or when it involves modifications of the way the technology works that were not agreed before. This topic of modification is tackled by Article 19 DCSD, which sets three cumulative conditions in order to modify the content and the service in a way that is fair to the consumer. Firstly, the contract must allow a valid reason for this modification, and, secondly, this modification must not entail further costs to the consumer and must be explained to them in a comprehensible manner[249]. Moreover, the consumer can terminate the contract in the event that said modification negatively impacts the use of this device[250].

The fourth interesting point about SDG and DCDS and home IoT objects is the part concerning remedies. Both directives take inspiration from the former Directive 44/1999/CEE[251] (which the SDG has repealed) and try to adapt it to a digital context. In particular, remedies for the lack of conformity in digital goods and in the provision of digital content follow a specific path. The first option is to return the item to conformity: the consumer can choose between repair and replacement if it is goods, whereas for digital content and services it is less clear how this should effectively be done (e.g., by deleting and downloading a content or service again through a trader-dedicated link?)[252]. If the return to conformity becomes impossible or the effort required is disproportionate, the seller or trader has a right to object to that. If that is the case, the consumer has the right to ask for a reduction of price or to terminate the contract[253]. As far as the termination of the contract, it seems that there are more elements to consider in the DCDS than in the SDG[254]. In the former, not only has the trader to reimburse what the consumer had paid originally, if applicable, but the trader is required to follow the principles of the GDPR[255]. More specifically, the trader will not use any content other than personal data which was provided or created by the consumer, and the consumer has the right to retrieve the digital content free of charge, without

[248] This in particular is one of the issues that the Green Deal and the New Consumer Agenda tries to fight also in light of a better environmental sustainability of the objects.
[249] It is an analogue of Article 12(1) GDPR
[250] Piia Kalamees, "Goods with Digital Elements and the Seller's Updating Obligation," *JIPITEC*, 12(2021)131-142.
[251] "Directive 1999/44/EC of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees *OJ L 171, 7.7.1999*, p. 12–16,' EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31999L0044.
[252] In particular, the right to ask for repair could be considered a more ethical and sustainable choice for the environment but, oftentimes, IP rights do not provide for asking for the repair of a device if not going to specialised centres which also result in being more expensive, therefore some authors wonder how this "sustainable choice" could be implemented given the actual state of things See Evelyn Terryn "A Right to Repair? Towards Sustainable Remedies in Consumer Law," *European Review of Private Law* 27,4(2019):851-873.
[253] Article 13 SDG and 13-14 DCDS.
[254] Article 13,14, 15, 16 DCDS.
[255] Article 16 DCDS.

hindrance from the trader, within a reasonable time and in a machine-readable format[256].

The final element on which to focus one's attention is that both the SDG and DCDS state that they are maximum harmonization directives[257]. Despite the fact that the contents of the recitals and definitions of both directives give an idea of coordination and uniformity, the area in which things are less stringent is the one concerning substantive liability rules and enforcement. MS can allow a period that could be shorter or greater than two years for the seller of an item with digital elements to be liable[258]. In the DCDS there is a similar rule of minimum two years for the lack of conformity to become apparent to establish the trader's liability. What is given here is an indication of a minimum requirement: the MS can set a higher threshold. Moreover, according to the DCDS, the MS can regulate consumers' liability claims towards a third party other than the trader "[…] *that supplies or undertakes to supply the digital content or digital service, such as a developer which is not at the same time the trader under this Directive*"[259]. Moreover, both directives are without prejudice (which means that they do not challenge) the national concepts about the formation, validity, effects and nullity of contracts[260]. Both directives had the limit of the 1 July 2021 to be translated effectively into national law and a review should take place in 2024[261].

However, it is likely that the lack of more uniform rules concerning enforcement and liability is the real "Achilles's heel of both directives": especially with regard to the liability of IoT objects, which are manufactured and their functioning monitored in several countries (some of which might not even be part of the EU). Innovators have increasingly fewer chances to compete in one or more MS and may not have the incentive to do so if enforcement rules differ from country to country. Nevertheless, it is also important to bear in mind that the actual set of competences between the MS and the EU does not allow anything other than that. A detailed explanation of how the competence to regulate private law liability will follow in chapter IV.

2.2.2. Analogue application and progressive adaptation

I. The adaptation of the already existent EU Consumer law to the digital revolution

In the second group of legislative acts that can be interpreted widely and in principle also be applicable to new technology, we find: the Unfair Commercial

[256] The reference to machine-readable format is Article 20 on data portability of the GDPR.
[257] Article 4 SDG and DSDC.
[258] Article 10(3) SDG.
[259] Article 9 SDG and Article 10 DSDC.
[260] Jorge Morais Carvalho," Sale of Goods and Supply of Digital Content and Digital Services – Overview of Directives 2019/770 and 2019/771," Journal of European Consumer and Market Law 2,5 (2019):194.
[261] Articles 24 and 24 in both the SDG and the DCDS.

Practices Directive (UCPD)[262], the Consumer Rights Directive (CRD)[263] and the Unfair Contract Terms in Consumers Contracts Directive (UCTD)[264].

Several scholarly works have been written about these legislative instruments, specifically with reference to the changes and the harmonization level that they have brought in the different MS legal order, however including it here would be outside the scope of this research. In the next subparagraph I will simply provide a summary of the main innovations that they each introduced.

Chronologically, the UCTD has been important in creating an orderly set of rules to establish whether a contractual clause is unfair to consumers by also relying on the concept of good faith, which is known under different names among EU members.

When it comes to the UCPD, there have been several important innovations: to create a list of practices that are always prohibited; to provide criteria on how to consider a practice unfair[265]; to maintain that consumers can be misled both through actions and omissions[266] and that both behaviours are not tolerable. Moreover, it sets the definitions and parameters of professional diligence, invitation to purchase and undue influence in these B2C contractual relationships[267].

Among other matters, the CRD has focused on the pre-contractual obligations and duties of traders towards consumers[268]. Moreover, it disciplined the consumer's right of withdrawal from said contract[269].

However, these important directives were drafted in a time (early 2000s) when Internet services and digital goods were not as widespread as the ones we use today. Therefore, consumers' associations and scholars alike have been discussing whether these directives could also be applied to online behaviours which could potentially mislead the consumers and/ or consistently limit their rights.

---

[262] "Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (Unfair Commercial Practices Directive) (Text with EEA relevance)
OJ L 149, 11.6.2005, p. 22–39," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32005L0029&qid=1661804213957. Hereinafter UCPD.

[263] "Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council Text with EEA relevance *OJ L 304, 22.11.2011*, p. 64–88," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32011L0083&qid=1661804079276. Hereinafter CRD.

[264] "Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts
OJ L 95, 21.4.1993, p. 29–34," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52003DC0702. Hereinafter UTC.

[265] Article 1 UCPD.

[266] Articles 6 and 7 UCPD.

[267] Respectively Articles 2 h), i) and j) UCPD.

[268] Articles 5, 6 CRD.

[269] Articles 9 - 16 CRD.

There had already been a guidance document on the interpretation of the CRD in 2014 and UCPD in 2016[270] in order to make them more suitable for the digital age. Following the 2017 REFIT procedure, it was decided that previous guidance documents were insufficient and therefore a new Amending directive EU/2161/2019[271] was approved. It should have been enacted by MS in 2022. This directive was approved shortly after the SDG and DCDS and, with them, constitutes an ambitious attempt to modernise EU Consumer law with a specific attention to the evolution of digital markets, as it is more evident than in the twin directives that data is considered to be a valid currency in order to obtain either a service or a good[272].

Directive 2161/2019 amended the UCTD, the UCPD and CRD. In the first it gave better guidance about penalties[273]. Most notably, UCPD's meaning of "product" will also extend to digital services and content[274]. Furthermore, terms such as "ranking" and "online marketplace" will be part of the updated UCPD [275]. Interestingly enough, also Annex I, concerning the "black list" of practices, is updated with practices that have become mainstream during recent years, such as "[p]*roviding search results in response to a consumer's online search query without clearly disclosing any paid advertisement or payment specifically for achieving higher ranking of products within the search results"*[276] and *"Stating that reviews of a product are submitted by consumers who have actually used or purchased the product without taking reasonable and proportionate steps to check that they originate from such consumers*"[277]. The CRD has also been amended. Most importantly, the notions of goods and content or services are updated to the ones of the SDG and DCDS[278]. Moreover, the terms "sales contracts" and "services contracts" are extended in their meaning to "*all kinds of contracts* [read also online ones] *which either transfer ownership to the consumers or any other contract where the trader "supplies or undertakes to supply a service" including a digital one*"[279]. New vocabulary from data protection is also present[280]. With regard to the field of application, it will be extended in

[270] "COMMISSION STAFF WORKING DOCUMENT GUIDANCE ON THE IMPLEMENTATION/APPLICATION OF DIRECTIVE 2005/29/EC ON UNFAIR COMMERCIAL PRACTICES Accompanying the document COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A comprehensive approach to stimulating cross-border e-Commerce for Europe's citizens and businesses SWD/2016/0163 final," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52016SC0163.
[271] "Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules (Text with EEA relevance) PE/83/2019/REV/1 *OJ L 328, 18.12.2019,* p. 7–28," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32019L2161. Hereinafter Dir. 2019/2161.
[272] Lavinia Vizzoni, *Domotica e diritto. La Smart Home tra regole e responsabilità* (Milano: Giuffrè 2021), 108-109.
[273] Article 1 Dir. 2161/2019.
[274] Article 3 (1) (a) Dir 2161/2019.
[275] Article 3 (1) (b) Dir 2161/2019.
[276] Article 13 (7) (a) (11a) Dir 2161/2019.
[277] Article 13 (7) (b) (23b) Dir 2161/2019.
[278] Articles 4 (1) (a) (3) and 4 (1) (d) (11) Dir 2161/2019.
[279] Article 4 (1) (c) (5),(6).
[280] Such as personal data in Article 4 (1) (b) (4a) Dir 2161/2019.

those instances " *where the trader supplies or undertakes to supply digital content which is not supplied on a tangible medium or a digital service to the consumer and the consumer provides or undertakes to provide personal data to the trader, except where the personal data provided by the consumer are exclusively processed by the trader for the purpose of supplying the digital content which is not supplied on a tangible medium or digital service in accordance with this Directive, or for allowing the trader to comply with legal requirements to which the trader is subject, and the trader does not process those data for any other purpose*"[281].

With the notices of 17 December 2021, and in the framework of the action of the New Consumers' Agenda[282], the Commission has given its green light to interpret these legislative acts in such a way that takes into account not of only one another but also the growing corpus of new legislation (GDPR, the SDG and DCDS): UCTD, UCPD and CRD traders/sellers must be in compliance with the GDPR and the E-privacy directive. Moreover, in the case of the CRD, the trader must provide "functionality", "interoperability" and "compatibility", terms that are taken from the SDG and DCDS[283]. With reference to the UCPD, it is interesting to notice that the false information regarding the environmental sustainability of a particular device (so-called "green washing") can be considered an unfair commercial practice in combination with Articles 6 and 7 UCPD[284]. The 2021 guidance documents replace the 2016 UCPD and the 2014 CRD ones respectively.

These directives and the various amendments and guidance documents will also turn out to be relevant for the domestic IoT: it is already the case that a consumer buys services or goods from their smart-phone or through the help of a smart TV. Navigating the contractual obligations and understanding if and when a consumer-user was also a victim of a misleading practice is likely to become more frequent, especially when the contract is concluded through a domestic IoT.

II. The New Approach and the New Legislative Framework Acts

Among the EU consumer law that could be applied to IoT nowadays we can find also the Product Liability directive (PLD) and the General Safety

[281] Article 4(2) (b) Dir 2161/2019.
[282] "COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL New Consumer Agenda Strengthening consumer resilience for sustainable recovery COM/2020/696 final," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0696. Hereinafter, New Consumer Agenda.
[283] "Commission Notice Guidance on the interpretation and application of Directive 2011/83/EU of the European Parliament and of the Council on consumer rights", 51-52, Accessed 31 January 2023, https://ec.europa.eu/info/sites/default/files/c_2021_9314_1_crd-guidance_en.pdf .
[284] "Commission Notice Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market," 93, Accessed 31 January 2023, https://ec.europa.eu/info/sites/default/files/c_2021_9320_1_ucpd-guidance_en.pdf .

Regulation (GSOD). The reason is that IoT objects for the smart home are designed and projected for the home, which, according to the EU law, should be the centre of economic interests of a subject who is not a professional. Moreover, these objects need to be safe, from a policy point of view, in order to encourage consumers to buy them and increase the free movement of goods in the Internal Market. A better assessment of the PLD and its history and structure, together with its fitness for IoT technology will be conducted in Chapter V. However, I considered it useful to present it concisely here.

The Product Liability Directive (PLD) has been one of the most challenged, but also long-living, instruments of the Consumer *acquis communautaire*[285]. Inspired by the evolution of product liability case law and scholarship in the US[286], the PLD can be considered as one of the first true examples of the so-called "New Approach"[287]. This was the legislative technique created in the '80s according to which the EU (then the EC) would dictate the main principles concerning the safety of a product or the objective requirements it had to meet[288]. The technical peculiarities were instead handled at a lower level by private or public, or public-private standard-setting organisations. In this way, it was thought that better governance would be achieved by collaborating not only with national authorities but also with the economic powers that had to enact specific sector-oriented regulations.

Before addressing the PLD in depth in Chapter V, it is important to introduce its main characteristics here. The PLD was one of the first and better functioning instruments that were underpinned by a risk assessment-oriented rationale: in a less complex, productive world than today's, this directive established some main points:

1) that the producer could not bear the responsibility for every malfunction of the object, especially if it had followed state of the art instructions. Moreover, once the product was commercialised, it was not reasonable to ask the producer to have meaningful control over its merchandise[289]
2) The notion of defectiveness of a product is a broad one: in the original wording, even the presentation could be susceptible to causing damages. Moreover, the term of comparison for the level of safety that is required by the product is based on what the consumer can reasonably expect[290].
3) This kind of liability was/is not based on fault. The producer is liable even if it did not intend to cause any harm, if the consumer could prove the

[285] Apart from one major modification (to exclude agriculture products from consumer products) it is still valid to this day in its form.
[286] Duncan Fairgrieve,Geraint Howells, Peter Møgelvang-Hansen et al.,"Product Liability Directive" in Piotr Machnikowski (ed) *European Product Liability : An Analysis of the State of the Art in the Era of New Technologies* (Antwerp-Cambridge-Portland: Intersentia, 2017), 19-23.
[287] Richard Neerhof, "The Use of Conformity Assessment of Construction Products by the European Union and National Governments: Legitimacy, Effectiveness and the Functioning of the Union Market," in *Certification, Trust, Accountability* Peter Rott (Cham: Springer Nature Switzerland, 2019) 76.
[288] Anna Wallerman, "Pie in the sky when you die? Civil liability of notified bodies under the Medical Devices Directive: Schmitt," *Common Market Law Review* 55(2018):265.
[289] This is starting to be questioned now, given that with sensors it is possible to always check on the device, theoretically. Joasia Luzak "A broken notion: impact of modern technologies on product liability," *European Journal of Risk Regulation* 11,3 (2020):631.
[290] Article 6 PLD.

causality link between the object and the damaging event. The producers can always exempt themselves from liability when one or more of the seven justification causes set out in Article 7 PLD[291] is met.

4) Property damage is also covered in addition to physical and life damage.[292]
5) This kind of liability does not formally exclude other regimes of liability, nor does it forbid the payment for immaterial damage[293]

Although the PLD has been challenged many times in court (even recently[294]), some argue that it is still a valid instrument[295] to be applied to the Internet of Things, or that at least some improvements must be carried out.

From a policy point of view, the Commission has set two groups for this purpose. The first one deals with the modernisation of the PLD itself. The second one, instead, focuses on Liability of new Technology in general, and it has already published an influential report on the liability of new technologies[296](see *infra* Chapter III, IV and V).

However, legal experts have begun to provide inputs regarding indications of what the update of the product liability directive should encompass. Some commentators believe that the definition of product in Article 2 PLD can already be applied to non-tangible material such as software[297]. This is also relevant for domestic smart objects, as software is the new aspect especially in "updated" consumer objects according to the novelty criterion, as explained in Chapter II. The meaning of "placing the product in circulation"[298] may also radically change, as it is now possible, thanks, for instance, to RFID technology, and other forms of tags, to monitor the product wherever it is located[299]. Moreover, especially in the case of a "main" IoT object and add-ons, or unbundled digital/tangible

[291] Exemption causes Article 7 PLD
[292] Article 9 PLD
[293] "Henning Veedfald v. Århus AmstKommune, Case C-203/99." EUR-Lex, Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A61999CJ0203&qid=1659524361571. Hereinafter *Veedfald*.
[294] See Section 2 of chapter V.
[295] Charlotte De Meeus, "The Product Liability Directive at the Age of the Digital Industrial Revolution : Fit for Innovation?," *Journal of European Consumer and Market Law* 29,4 (2019):149-154.
[296] Expert Group on the Liability of AI and New Technologies, *Liability for Artificial Intelligence and other emerging digital technologies* (Brussels:2019) https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2020/01-09/AI-report_EN.pdf ,
[297] In particular, some argue that while it can be technically possible to already include data and damage to data, hence software within the present text of the PLD, this would not however reflect the original intentions of the drafters See Bernard A. Koch "Product Liability 2.0- Mere Update or New Version?," In *Liability for Artificial Intelligence and the Internet of Things Münster Colloquia on EU Law and the Digital Economy IV*, Sebastian Lohsse, Reiner Schülze and Dirk Staudenmayer (Baden-Baden: Beck Nomos,2020)103. Of this opinion, but by focusing more on the legal qualification of software see Ernst Karner, "Liability for Robotics: Current Rules, Challenges and the Need for Innovative Concepts", in *Liability for Artificial Intelligence and the Internet of Things Münster Colloquia on EU Law and the Digital Economy IV*, Sebastian Lohsse, Reiner Schulze et Dirk Staudenmayer (Baden-Baden: Beck Nomos,2020),119.
[298] Articles 6 (c) and 7 (a)
[299] Joasia Luzak, "A broken notion: Impact of modern technologies on product liability," *European Journal of Risk Regulation* 11,3 (2020):630-649.

components, there will be an increasing need to clarify whether the consumer can sue the various producers for the damage created by the unbundled object or service, which could be covered by the PLD (for instance physical damage), or whether it would be just the producer of the object that guaranteed "compatibility" with other IoT objects or services. The answer is simple if the unbundled part is a tangible object, as the PLD will be applicable to the producer of the tangible part. However, the situation may be more complex if the added component provides a service. The SDG DCDS can certainly be applied, but, as far as they are phrased, it depends on whether the sales contract has stated or not that there are pre-installed applications or software programmes or not[300]. In any case, the application of these directives does not cover damages to physical integrity and property, which are dealt with by Article 9 PLD.

Furthermore, one of the other matters that could be clarified, especially by the Modernising Committee is what could be considered as immaterial damage according to the new PLD. For instance, it must be taken into consideration that a smart thermostat is potentially easily hackable and said hack could give rise to loss of property. This could give a consumer the right to use the PLD against a defective smart thermostat producer and ask for compensation for the damage caused to their property by the theft which was enabled by the instrument[301], and also for the state of anxiety that the trauma left on them.

If the PLD was the symbol of the new Approach, the next step in co-regulation at the EU level is represented by The General Security of Objects Directive, which could also be applied to IoTs[302]. It is a horizontal directive, meaning that wherever there is no specific *ad hoc* legislative act (be it a directive or a regulation), it can be applied[303].

It creates a framework where the Commission, the traders, the Member States and EU citizens can collaborate in maintaining a sufficiently high standard of object safety.

The GSOD is connected to the PLD in several ways, despite the fact they are applied to two different fields: the PLD to private law liability and the GSOD to compliance and administrative liability, which could also entail the PLD[304]. In the PLD, safety is mentioned in Article 6 but it is connected with general parameters to measure it such as its presentation, the use that is expected of it and what it does, and the time when it was placed into circulation. However, this

[300] See previous part on DCDS and SDG.
[301] For instance, thieves understand from the average temperatures in the rooms of the house whether there is someone or not and decide to rob the consumer home when they are not there. This actually already happened. Aaron Tilley, "How Hackers Could Use A Nest thermostat As An Entry Point Into Your Home," *Forbes*, March 6, 2015, https://www.forbes.com/sites/aarontilley/2015/03/06/nest-thermostat-hack-home-network/.
[302] "Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety (Text with EEA relevance) OJ L 11, 15.1.2002, p. 4–17," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32001L0095.
[303] Recital 5 GSOD.
[304] Cristina Amato, "Product Liability and Product Security: Present and Future," In *Liability for Artificial Intelligence and the Internet of Things Münster Colloquia on EU Law and the Digital Economy IV*, Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (Baden-Baden: Beck Nomos,2020),77-95.

list is not limited to these conditions, as in the same article the mention of "*all the circumstances taken into the account*"[305] is explicit. This means that other sources of safety obligations could be considered, hence the connection with the GSOD. The GSOD is therefore a legislative act that is at a crossroads with consumer protection and administrative law.

Hopefully, the recently approved regulation on the General Safety of Products (GSP) will help achieve this objective in the future [306]. This seems to be the case, as it provides a definition of product (Article 3(1)) which is almost exactly the description of an IoT object.

Nevertheless, the GSOD could already be relevant for the domestic IoT market, as smart home objects are slowly but steadily being normalised and becoming more accessible. In most cases, a small plug or a remote control will have fewer safety risks than a complex alarm system or a smart fridge. In Chapter II, it was explained that the majority of the objects that are marketed as "consumer-friendly" are not technologically hyper complex. Nevertheless, safety standards and safety rules for them have not yet been fully harmonised. Further, the GSOD could partly influence consumer law because " *i) when it refers to the definition of products, it mentions that this definition applies regardless of whether or not it was intended for consumers*[307] *and ii) when listing the elements that a product has (or is presumed to have) to reach the required conformity level, there are not just the state of the art but also reasonable consumer expectations among other elements*"[308]. One difference in comparison with the PLD is that the definition of producer is wider and more articulated, as it also includes *"[…] other professionals in the supply chain, insofar as their activities may affect the safety properties of a product;"*[309] Also, the concept of product is quite extended and can encompass services[310].

The reasons for which the GSOD can be considered as part of administrative law is that it deals with the Commission asking national or European SDOs (Standard Developing Organisations, see chapter II) to create safety standards, and it requires producers that create low-risk objects to abide by those standards, also because the final result is a conformity assessment that is obtained through the work of private bodies with administrative functions. Generally, the standards requested and approved by the Commission are the ones that are made mandatory in national law and therefore become national technical regulations. For the lower risk category of objects, the producer must abide by the standards and certify that its product is of the correct standard. The Member states must also check whether standards are respected. All these

[305] Article 6 PLD.
[306] "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council, and repealing Council Directive 87/357/EEC and Directive 2001/95/EC of the European Parliament and of the Council," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0346&rid=8.
[307] Article 2(a).
[308] Article 3 (3) (f).
[309] Article 2(e) (iii).
[310] Article 2 a).

different actors and citizens are connected also by a common rapid alert and recall of products system (RAPEX).

The Medical Devices Directive (MDD)[311] and Medical Devices Regulation (MDR)[312] follow this mixed approach of administrative law and compliance of the New Legislative Framework (the update of the New Approach), but they specifically apply it solely to medical devices. The rationale behind this legislation was to classify medical devices into several classes depending on the level of harm they might cause. For each category of devices (four in total named I, II a, II b and III)[313], a series of technical and standardised procedures were specified, in order not only to ensure the highest possible level of safety but also to manage the inherent risk in some of these devices. In order to understand how to classify a medical device according to its level of risk and the procedure to be followed, one had to go back and forth from the recital and operative part to the annexes. In this specific case, one had to combine Article 9 MDD, which concerns the different classes, with Annex IX, which is about the classification rules, and with Article 11 MDD on the rules of the different procedures and then Annexes II, III, IV, V or VI according to the procedure established by Article 11 MDD.

For some devices which might entail more risk, it was necessary that extra precautions be taken. The procedures to evaluate the conformity of the medical devices were carried out through Notified Bodies (NB), private, public or public private entities chosen by the MS and notified to the Commission as EU certifiers of the conformity of medical devices. As already cited in Chapter II, the directive was not founded on a system of pre-approval, as is the case in the US with the FDA system[314], but the producer of implantable devices (such as prostheses in the famous PIP scandal) had to certify it had followed state-of-the-art guidelines and that a series of audits then followed. Despite an audit procedure in principle being more dynamic than a certification procedure[315] , this did not prevent the Notified Body in some cases (such as TÜV France) from being negligent, as noticeable irregularities were made also at an accounting level[316] and there was no reaction from the NB.

In order to prevent other medical devices scandals, the MDR was introduced. A comparative analysis with the MDD shows that several pillars of

[311] "Council Directive 93/42/EEC of 14 June 1993 concerning medical devices *OJ L 169, 12.7.1993, p. 1–43, "*EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31993L0042.

[312] "Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Text with EEA relevance.)*OJ L 117, 5.5.2017, p. 1–175*,"EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R0745 .

[313] Recital 19 MDD and Article 9 MDD and Annex IX MDD.

[314] Holly Jarman, Sarah Rozenblum and Tiffant J. Huang, "Neither protective nor harmonized: the crossborder regulation of medical devices in the EU," *Health Economics, Policy and the Law* 16,1 (2021):51-63.

[315] Gerrit Hornung and Stefan Bauer, "Privacy Through Certification?: The New Certification Scheme of the General Data Protection Regulation," In *Certification Trust Accountability*, Peter Rott (Cham, Switzerland: Springer, Nature 2019),115.

[316] The quantity of the gel that had to be used for the prosthesis was inferior to the amount that needed to be purchased.

the previous directive are still present in the MDR. The structure of the MDR is the same as the MDD: there is a longer list of recitals, followed by general rules or principles that must be integrated with the details of the annexes. Surprisingly, the rules on classification in the new Annex VIII are still those from the old Annex XI, in addition to the classes of risks, and they still have the same nomenclature (I, IIa, IIb and III). All conformity procedures are in Annexes IX, X and XI. They are all inspired by the previous procedures in the MDD annexes. Furthermore, the system based on NBs is still in place.[317] There are new, more detailed rules on how the MS must select them and there are also more rules concerning the interaction of standards (harmonised, *ad hoc* or more general) with the MDR itself[318]. There is a new list of post-market surveillance duties[319] and, finally, a harmonization of the rules on clinical investigations[320]. There are a few new items concerning the liability theme at large, clearly originating from the issues highlighted by the PIP saga.

The first one is that the manufacturer of medical devices should have formal obligations according to Article 10 MDR. Among these, there is the obligation to: "[…] *in a manner that is proportionate to the risk class, type of device and the size of the enterprise, have measures in place to provide sufficient financial coverage in respect of their potential liability under Directive 85/374/EEC, without prejudice to more protective measures under national law*".[321]

The second new rule introduced by the MDR to consider for present purposes is that NBs will be supervised by an independent authority based in each Member State[322]. Even so, NBs will be held liable for the activities of subsidiaries and subcontractors in issuing the conformity certifications required for specific classes of medical devices[323]

It is important to bear the structure of these two legislative acts in mind as they will apply also to health IoT that can be used in the home, such as monitoring vests for medical consultation or exergames in front of a smart TV with monitoring devices for the body[324].

3. Platform regulation and the IoT

3.1. The E-commerce Directive and the proposed Digital Services Act (DSA)

Up to this point, I have applied the analysis of EU law by considering IoT home objects as physical products with integrated software. However, some of the most important domestic IoT objects are also becoming preferred gateways to reach platforms and services, such as our smartphones or voice assistants.

[317] The system is extensively detailed in Chapter IV of the MDR and in its Annex VII.
[318] Article 8, 9 MDR.
[319] Annex XIV MDR.
[320] Annex XV MDR.
[321] Article 10(16) MDR.
[322] Article 35 MDR.
[323] Article 37 MDR.
[324] More on this discussion can be found in Chapter V, subsection 2.3 on medical devices.

Until recently, it was the task of the E-Commerce Directive[325] to discipline the role of Internet Service Providers (ISP), which were the "ancestors" of the system of platforms and search engines that are now also accessible through some domestic smart objects[326]. The E-Commerce directive connection to the home IoT consists of the system of exemptions to liability that is codified in Articles 12, 13 and 14. Depending on the typology of the ISP (which could be mere conduit, caching and hosting), the extension of the ISP's obligations in order to be exempt from liability varied according to the control these ISPs had on the content and type of service that they made available to the general public[327].

However, the E-Commerce directive rules on the exemption of liability will not stay in the same directive for long. As a part of the EU's Digital Strategy, the Digital Services Act (DSA)[328] was presented in 2020. It is a regulatory instrument

[325] "Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)**,** *OJ L 178, 17.7.2000, p. 1–16*," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32000L0031. DSA finds its rationale in Article 114 TFEU, concerning the harmonization of the internal market.

[326] For instance, think of a smart-tv that gives access to streaming platforms. To know more about the evolution of the platform business system, see Silvia Martinelli, "La responsabilità delle piattaforme di intermediazione," in *LA RESPONSABILITÀ CIVILE NELL'ERA DIGITALE (Atti della Summer school 2021)* Valentina V. Cuocci, Francesco Paolo Lops, Cinzia Motti (Bari: Cacucci editore, 2022), 267-282.

[327] If we analyse the E-Commerce rules on liability (respectively Articles 13-14-15 of the directive), there is a distinction between several kinds of ISPs: the ones which function are only mere conduit (12), caching (13) and hosting (14). According to their level of control and involvement over the content and the service, the exemption from liability is more or less extended. If an ISP just "[…] *provides mere conduit, meaning that it transmits in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, the provider is not liable unless it initiates the transmissions, or does not select the receiver of a transmission and does not act to either select or modify the information which is transmitted*" (Article 12). It is interesting to notice that already in the directive there is a perfect equivalence between mediated and automatic transmission. Instead, the caching provider "[…] *stores information, even temporarily, both with automated or non-automated means. It will not be liable provided that a) does not modify the information; b) it complies with the conditions to access to the information; c) the provider complies also with the rules of the updating of the information which must be done in a way that is well-recognised by the industry, d) it does not interfere with the lawful use of the technology and, most importantly e) that it must remove or disable access to the information at the initial source because it was a content that was removed from the original source or an administrative authority or court has asked to take it down* […]"(Article 13). Lastly, the hosting services are maybe more known because of landmark cases that they were part of and that were judged by the CJEU such as with the famous *L'Oréal* case. Hosting services (Article 14) are different from the other ones has they can have more control on the content and information that they showcase. In fact, hosting services are not liable only in two cases "[…] *the provider does not have actual knowledge of illegal activity or information and, as far as claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent*"(Article 14). In addition, if the provider obtains knowledge of illegal content it must act "expeditiously" in order to remove or to disable the access to information. "L'Oréal SA and Others v eBay International AG and Others, Case C-324/09," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62009CJ0324. More on these themes, Stefano Alberti, "L'altra faccia dell'ISP liability. La responsabilità contrattuale del cloud provider fra legge, usi e condizioni negoziali," *Giustizia Civile* (2014): 1-16.

[328] "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC COM/2020/825 final," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN . On 27th October 2022, the Digital Services Act was published in the Official Journal of the EU. "Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance) PE/30/2022/REV/1 *OJ L 277, 27.10.2022, p. 1–102*," EUR-Lex, Accessed 31October 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=1666972131568.

which will concern the global providers of services also operating in the EU. The agreement on the text was reached with the Council on 18 July 2022 [329]. In this context, Articles 12, 13, 14 will become the new Articles 4,5 and 6 DSA.

Nevertheless, it will not be a generalised set of measures. One of the DSA's main innovations is the introduction of a complex set of due diligence requirements on all those online service providers that fall under the definition of VLOPS (Very Large Online Platforms) and VLOSEs (Very Large Online Search Engines) in addition to the former E-Commerce liability rules. To fall within the VLOPs and VLOSEs categories, the online search platform or service must have a number of 45 million active users or higher each month[330].

On their end, scholars do not seem optimistic about the efficiency of combining the E-Commerce liability rules and the complex set of duties that will need to be applied to VLOPs and VLOSEs as, in some cases, they will be even more shielded from liability issues[331] . Moreover, the fact that there no effective remedies for misleading information and unsafe products within the text is also considered a missed opportunity[332].

3.2. The Digital Markets Act (DMA)

Although this thesis does not focus on platforms, it is worth mentioning the main characteristics of the Digital Markets Act (DMA)[333] and its connection to IoT objects for the home as it will be relevant in order to understand Chapter VI on the US regulatory approach to digital technologies and platforms. This regulation complements Articles 101 and 102 TFEU on competition in the internal market, by giving the Commission powers to monitor and sanction the platform and internet services that are most likely able to influence access to digital markets. Its functioning mechanism consists of the imposition of compliance duties on those entities that are able to influence access to digital markets: the gatekeepers[334]. The agreement between the Council and the European Parliament was reached in July 2022, on the same day of the agreement on the

[329] Thierry Breton, "Sneak-peek how the Commission will enforce the DMA and DSA", Linkedin Post, July 6, 2022, https://www.linkedin.com/pulse/sneak-peek-how-commission-enforce-dsa-dma-thierry-breton https://www.consilium.europa.eu/en/press/press-releases/2022/04/23/digital-services-act-council-and-european-parliament-reach-deal-on-a-safer-online-space/.
[330] Recital 76 DSA Article 33 DSA.
[331] Sara Tommasi, "The Liability of Internet Service Providers in the Proposed Digital Services Act," *European Review of Private Law* 6(2021): 925-944.
[332] Christoph Busch and Vanessa Mak, "Putting the Digital Services Act into Context: Bridging the Gap between EU Consumer Law and Platform Regulation," *Journal of European Consumer and Market Law* 3(2021): 109-115.
[333] "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on contestable and fair markets in the digital sector (Digital Markets Act) COM/2020/842 final," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A842%3AFIN . The DMA was finally voted and approved into applicable EU law at the end of
[334] Article 3 DMA.

DSA. It was finally published into the Official Journal last 12th October 2022[335]. These regulations in fact were presented together as complementary. The DMA connection to the home IoT objects is similar to that of the DSA: it interests some of them as they are an interactive gateway to platforms.

The reason for regulating digital markets from a competition and administrative point of view through the DMA is the same as for the DSA, but seen not from the angle of provision of content or services, but of market power. Global commercial entities, which have become essential in the evolution of the contemporary Internet structure, often by using platform structures (not exclusively), have created digital environments that give the possibility to millions of people and businesses to interact with each other. They have become *de facto* essential, and users have become dependent on them. In fact, both consumers and (small) business users use these platforms. These entities can actually unilaterally grant or deny access to their internet services, that is why the most prominent of them are called gatekeepers. On several occasions, it was alleged that these entities had created several issues for business and consumer users. Some of these conducts or omissions configured situations of abuse of power by the owner of the platform/service towards both consumers and businesses users. Some examples could be, for instance, creating different access conditions for business users, "stealing" ideas from business users to create similar products or services and make them more convenient for purchase (self-preferencing)[336]. The EU Commission actively challenged these situations in several litigation procedures, some of which are still ongoing[337].

In order to change this situation, the EU regulatory powers and the EU legal experts managed to find an agreement about the fact that the two fundamental Articles of the TFEU concerning private competition enforcement (meaning Articles 101 and 102 TFEU) were not sufficient, as they were remedies acting only *ex-post*. Instead, a regulatory *ex-ante* instrument was thought to be more efficient for digital markets, in combination with the previously cited TFEU articles. One of the main reasons why Article 101 and 102 TFEU were no longer considered sufficient was that they were (and are still) general and flexible clauses, which were not created at a time when digital ecosystems were as developed as they are nowadays and are time-consuming to apply. In fact, it takes years between the Commission's notification about the investigation opening for either an alleged anticompetitive agreement/practice (Article 101

[335] "Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance)
PE/17/2022/REV/1 OJ L 265, 12.10.2022, p. 1–66", EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925&qid=1674037261043.
[336] Filomena Chirico, "Digital Markets Act: A Regulatory Perspective," *Journal of European Competition Law and Practice* 12,7 (2021): 493.
[337] Such as the "Google Alphabet v. Commission (Google Android), Case T-604/18", CURIA, Accessed 31 January 2023, https://curia.europa.eu/juris/liste.jsf?num=T-604/18 (still ongoing).
See also Rupprecht Podszun, Philipp Bongartz and Sarah Langestein, "The Digital Markets Act: Moving from Competition Law to Regulation for Large Gatekeepers," *Journal of European Consumer and Market Law* 2(2021):65.

TFEU) or an alleged abuse of dominance (Article 102 TFEU) one and a final judgment by the CJEU.

Hence, in order to evaluate whether a company is a gatekeeper, which means that it is a subject responsible for granting access to a platform or service according to Article 3 DMA, there is a two-step test to follow. Firstly, the company must be a Core Platform Service (CPS), hence it must fulfil the subjective criteria of Article 2 DMA. Secondly, in order to identify the gatekeeper, Article 3 DMA provides for three main cumulative criteria which concern: *i)* the gatekeeper size that must impact the internal market (Article 3(1)(a) DMA)[338], *ii)* the control of an important gateway for business users towards final consumers (Article 3(1)(b) DMA) [339] and, finally, "*an entrenched durable position*" now or in the foreseeable near future (Article 3(1)(c)[340]. Briefly, the quality of gate keeper is measured on both qualitative and quantitative elements[341].

The DMA will subject gatekeepers to a notification obligation towards the Commission if they already meet or will meet the combination of qualitative and quantitative criteria in the near future[342]. Alternatively, the Commission can always decide that a certain entity meets the previously stated requirements[343]. Especially the quantitative requirements are rebuttable presumptions. This initiative has been welcomed by scholars as an important development in the creation of fair and contestable set of rules in the most prominent and famous digital environments.

However, some critical remarks might involve the fact that the two abstract principles, which are the rationales of the proposal (market contestability and fairness) are still rather general and could benefit from further structuring, as suggested by some scholars[344]. Moreover, in its two most interesting articles, Articles 5 and 6 DMA, the Commission seems to have drawn up a list of practices that were actually taken from previous competition case law. Scholars and legal practitioners who are well-versed in competition and antitrust issues could easily spot them[345]. The self-executive character of these clauses means that, unlike in

[338] Which means that there is the presumption of impacting the market whenever it achieves an annual turnover in the European Economic Area (EEA) equal to or above 7.5 billion in each of the last financial three years or where its average market capitalisation or equivalent fair market value amounted to at least €75 billion in the last financial year, and it provides a core platform service in at least three Member States. This is the text after the Council agreement, in the original proposal the threshold was 6.5 billion. Article 3(2)(a) DMA.

[339] This is presumed to be the case if the company operates a core platform service with more than 45 million monthly active end users established or located in the EU and more than 10,000 yearly active business users established in the EU in the last financial year. Article 3(2)(b) DMA.

[340] This is presumed to be the case if the company met the other two criteria in each of the last three financial years. Article 3(2)(c) DMA.

[341] Rupprecht Podszun, Philipp Bongartz and Sarah Langestein, "The Digital Markets Act: Moving from Competition Law to Regulation for Large Gatekeepers," *Journal of European Consumer and Market Law* 2(2021): 63.

[342] Article 3(3) and (4) DMA.

[343] Article 3(3) and (4) DMA.

[344] Prodszun Philipp Bongartz and Sarah Langestein, "The Digital Markets Act: Moving from Competition Law to Regulation for Large Gatekeepers," *Journal of European Consumer and Market Law* 2(2021): 62.

[345] Cristina Caffarra and Fiona Scott Morton," The European Commission Digital Markets Act: A translation," *VOXEu CEPR*, Available:https://voxeu.org/article/european-commission-digital-markets-act-translation, Accessed 27 May 2022.

Article 101(3) TFEU[346], according to which the Commission and the undertaking (the business company in competition law parlance) can bring forward justifications for the alleged anticompetitive practices, it will no longer be possible to evaluate these justifications when the DMA applies. Moreover, it is still unclear how the DMA will be enforced out by the Commission alone, given the fact that the European Network of Competition authorities is not mentioned.

In any case, the DMA is a regulatory model also able to inspire the US. Specifically, Chapter VI will explain how the DMA would play a role in the US Congress bipartisan decision to regulate platforms and search engines through antitrust law (the equivalent of competition law in the US).

4. More technical policy and legislative documents

The main theme of this part of the chapter is how the development of cybersecurity policies and regulations is going to impact the IoT objects for the home and what the interconnections are between cybersecurity and EU private/consumer law. With regard to cybersecurity, there are already three existing legislative acts (the Network Information Systems and the European Electronic Communications code) that are already applicable to domestic IoT objects.

It is important to summarise the main way in which cybersecurity rules interact with the domestic IoT for potential consumers. Even if the terms safety and security are not the same[347], it is quite apparent that they are going to influence each other. In fact, a better level of cybersecurity of a home IoT object will also influence the safety that one can expect from that object, which is relevant not only for the PLD but also for the SDG.

4.1. The EECC, NIS and NIS 2: what they mean for the home IoT

The EECC repealed the pre-existent directive 21/2002/EC, which is interesting for domestic IoT for several reasons. Firstly, it defines what an electronic communications network is. This definition could also be a description of an IoT system as the definition of electronic communications networks can be described as: "[…] *transmission systems, whether or not based on a permanent infrastructure or centralised administration capacity, and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including internet) and mobile networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television*

[346] Filomena Chirico, "Digital Markets Act: A Regulatory Perspective," *Journal of European Competition Law and Practice* 12,7 (2021):495.
[347] In fact, the former belongs to the administrative-private regulatory part of EU law, while the second one mainly concerns technical discipline.

networks, irrespective of the type of information conveyed"[348]. This is quite an encompassing definition, which is very similar to the description of IoT we have given in Chapter I, but is too general as it also covers public structures, an area that is outside the scope of this work. As far as definitions are concerned, the meaning of consumer is interesting because of two elements: the first one is a "classical" EU consumer law part, which means that it is applicable to a natural person who acts outside their business craft and profession. The second part is borrowed from the definition of user[349]. This is a new approach in defining stakeholders in technology. In Chapter IV, I will explain further why the definition of consumer, data subject and user is gradually blending into a mixed one.

Secondly, the EECC promotes the creation of better connectivity and access to fixed or mobile networks[350] in order to grant EU citizens a wider access to electronic communications services[351] and, by consequence, to create also interconnected environments, such as the smart home, easier and faster. It aims to reach this objective through harmonization measures such as non-compulsory standards indicated by the Commission on the Official Journal[352].

However, the relevance of the EECC for this thesis is that it has interconnections with the DCDS, especially in bundle contracts. These kinds of contracts are actually widespread and may involve a home IoT object. Imagine a mobile telephone operator that also provides an internet box, which is also connected to a smart television, all in the same contract. Technically, this contract is defined as a bundle contract as it groups together different goods and services. As a rule, the DCDS should not overlap with the EECC given that Article 3(5)(b) formally excludes it[353]. Sein, however, rightly points out that the EECC definition of Over The Top provider (OTT), or better, number - independent interpersonal communications services coincide with the scope of Article 3(5)(b), as this article makes an exception for number- independent interpersonal communications[354]. This creates a discrepancy in remedies for consumers: if the service is a number-independent communications service, the solutions already explained concerning the lack of conformity in the DCDS will apply, and providers will be subject to EU and national law rules on contractual liability[355]. On the other hand, if the service is number-dependent, consumers cannot rely on the set of DCDS

[348] Article 2(1) EECC.
[349] The general definition of user is wider than the one of consumer in the EECC because it also involves legal persons. Article 2(13) EECC.
[350] 3(2)(a) EECC.
[351] 3(2)(d) EECC.
[352] Article 39 EECC.
[353] Karin Sein, "Interplay Of Digital Content Directive, European Electronic Communications Code And Audiovisual Media Directive In Communications Sector," *JIPITEC* 12,1 (2021): 170.
[354] Karin Sein, "Interplay Of Digital Content Directive, European Electronic Communications Code And Audiovisual Media Directive In Communications Sector," *JIPITEC* 12,1 (2021): 170.
[355] Karin Sein, "Interplay Of Digital Content Directive, European Electronic Communications Code And Audiovisual Media Directive In Communications Sector," *JIPITEC* 12,1 (2021): 175.

solutions[356]. However, they could still rely on Article 105(4) EECC, which gives users the right to terminate the service[357].

The NIS Directive is a minimum harmonization[358] instrument which served the purpose of pushing MS to adopt national cybersecurity national strategies[359]. It is coordinated by a Cooperation Group[360] whose function is to exchange relevant information about the safety and security of network systems. NIS distinguishes these network systems by placing them in three typology groups. These three typologies of network systems all seem to refer to the general definition of IoT given in Chapter I. For instance, the following is considered a network system "…*(a) an electronic communications network within the meaning of point (a) of Article 2 of Directive 2002/21/EC*[361] *;(b) any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; or (c) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance* […]"[362]. The network systems security is instead defined as "[…] *the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems*"[363]. Coming back to the NIS I, the national cybersecurity strategies had to have the creation of one or more national Computer Security Incident Response Teams (CSIRTs) as an objective. These were supposed to cooperate in a network [364], especially in cases where there were supposed to be significant disruptive effects[365].

It is important to point out that this directive entered into force only a few months before the approval of the GDPR: the actual text still recalls the function

[356] Karin Sein, "Interplay Of Digital Content Directive, European Electronic Communications Code And Audiovisual Media Directive In Communications Sector," *JIPITEC* 12,1 (2021): 175.
[357] Karin Sein, "Interplay Of Digital Content Directive, European Electronic Communications Code And Audiovisual Media Directive In Communications Sector," *JIPITEC* 12,1 (2021): 175.
[358] Article 3 NIS.
[359] Article 1(2)(a) NIS.
[360] Article 10 NIS.
[361] Directive 2002/21/EC was the document repealed by the electronic communications code. In Article 2(a) it reads that *"… an electronic communications network means transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed*." Now EECC.
[362] Article 4(1) NIS.
[363] Article 4(2) NIS.
[364] Article 12 NIS.
[365] A significant disruptive effect is defined as such by taking into account several factors such as *"…(a) the number of users relying on the service provided by the entity concerned; (b) the dependency of other sectors referred to in Annex II on the service provided by that entity; (c) the impact that incidents could have, in terms of degree and duration, on economic and societal activities or public safety; (d) the market share of that entity; (e) the geographic spread with regard to the area that could be affected by an incident; (f) the importance of the entity for maintaining a sufficient level of the service, taking into account the availability of alternative means for the provision of that service…"* but also sector specific elements. Article 6NIS.

of the DPD in Article 2 and most of its definitions, including the one regarding standard, are connected to the directive on information society services[366]. Nevertheless, the NIS is still the directive in which there is at least the description of several IoT components for the home such as the cloud computing service[367]. Another noteworthy element is that one of the tasks for the MS is to promote the adoption of either European or international standards without discrimination or imposition of a particular kind of technology in order to enforce technology neutrality[368]. The last important characteristic of this first NIS directive is the definition of risk: it is described in a rather technical way as *"…any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems*…"[369]. Another important role is taken up by ENISA, the EU agency for cybersecurity, that should help in making the selection of technical standards easier for MS[370].

This lack of connection of the NIS with the GDPR and the EECC is one of the reasons why a new proposal about an update of the NIS directive (called NIS 2)[371] has recently been approved. However important, the abovementioned reasons for the update of the NIS directive are not the most relevant ones: being a minimum harmonization directive, the implementation of the NIS was more difficult than accounted for. The end result was a fragmentation of the digital single market[372], and the difficult integration with newer legislative acts involving technology is proving more and more difficult, with the NIS functioning as a *lex generalis*[373]. As described in the proposal, the main implementation of the NIS II directive will focus more on " *the processes of cooperation and governance, by*

[366] Article 2 NIS.
[367] Article 4(19) NIS.
[368] Article 19 NIS. The definition of standard in the NIS, however, is taken from Article 1(1) or the Standardisation Regulation 1025/2012 in which standards are defined as technical specification adopted either at a national, EU harmonization, European standard or International body level. Regulation 1025/2012. "REGULATION (EU) No 1025/2012 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 October 2012
on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council
(Text with EEA relevance), *OJ L 316, 14.11.2012,* p. 12–33," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32012R1025.

[369] Article 4(9) NIS.
[370] Article 19(2) NIS.
[371] "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union *OJ L 194, 19.7.2016, p. 1–30*," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148&qid=1661692299067.
[372] European Parliament, "The NIS 2 Directive: A high common level of cybersecurity in the EU December 2021," Accessed 04 February 2022, https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333.
[373] In particular, Ducuing explains that the text of Article 1(7) NIS should be a *lex generalis* and should not be applied whenever sector-specific EU requirements apply, provided that they are *at least equivalent* (emphasis added). This least equivalence criterion is contributing to create confusion especially with new sector specific technologies regulation such as the Cooperative-Intelligent Transport Systems Regulation (C-ITS). Charlotte Ducuing, "Understanding the rule of prevalence in the NIS directive: C-ITS as a case study," *Computer Law and Security Review* 40 (2021):105514-105516, https://doi.org/10.1016/j.clsr.2020.105514.

"*adding more stakeholders accountable for compliance instead of implementing measures on standardisation and introducing a new distinction between private and public important and essential entities*"[374] "*It will still however be applicable to IoT objects*" (including the domestic ones)[375]. Both Parliament and the Council agreed to the proposal with minor amendments[376]: Parliament "*insisted more on adding public essential entities and providing rules on data sharing, whereas the Council insisted more on the relationship of the NIS 2 with sector-specific legislation by maintaining the criterion of the least equivalence and by adding that the physical and environmental security of NIS should be protected*"[377]. All these measures will be complemented by the newly announced Cyber resilience regulation which should create a horizontal framework to harmonise cybersecurity standards in the EU[378].

5. The long path to AI (and its liability) regulation: consequences for domestic IoT objects.

AI is not the first new generation technology to receive full attention from the EU institutions. In 2009 the Commission published a document concerning the importance of the IoT, which set a roadmap for its adoption and for the development of a mature market for this technology[379]. This also prompted the former 29 Article Working party to release a document concerning the risks for data protection caused by the development of this technology in 2014[380]. In these documents the IoT was seen as an evolving technology that would develop from a simple array of sensors and actuators to the creation of more autonomous objects, which in turn would create connected environments able to bring forward different fields. Specifically, the 29 Working Party warned about challenges such as: "[…] *the lack of control on the object and the condition of information asymmetry of the user of the device on how the object concretely operates; the quality of the users' consent as the user is not always aware of when and how the data processing is operating; the intrusive bringing out of behaviour patterns and profiling; the limitations to stay anonymous when using services and the*

[374] Article 2 of the Proposal NIS2.
[375] Article 2 (2) (a) (i),(ii) (iii) of the Proposal NIS 2.
[376] The NIS II directive was finally published on 27th December 2022. "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) PE/32/2022/REV/2, OJ L 333, 27.12.2022, p. 80–152", EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/eli/dir/2022/2555.
[377] Anna Baldin, "EU: Towards the adoption of the NIS 2 Directive," One Trust Data Governance, December 2021, Accessed 31 January 2023, https://www.dataguidance.com/opinion/eu-towards-adoption-nis-2-directive.
[378] "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 COM/2022/454 final," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0454.
[379] European Commission, "Internet of things. An action plan for Europe", 2009, Accessed 04 February 2022, http://ec.europa.eu/information_society/policy/rfid/documents/commiot2009.pdf%.
[380] Article 29 Data Protection Working Party, "Opinion 8/2014 on the on Recent Developments on the Internet of Things", 2014, Accessed 31 January 2023. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm . Hereinafter, Opinion 8/2014.

cybersecurity risks of these objects"[381]. These are all features that create a link with the main argument at the beginning of the chapter: that processing and data protection will always be present in the new legal and policy developments for technology and will impact rules on the liability of these complex systems[382].

As thought at the start of its history, the IoT was actually part of domotics, that was the name used for that discipline that was placed somewhere between automation, electronic engineering and architecture/interior design, and whose objective was the creation of objects for a fully automated home. These premises were based on the Machine 2 Machine technology principles, and in general, on Weiser's paradigm of ubiquitous computing[383]. If we take the most modern definition of robots as objects that are able to be autonomous and perform several kinds of tasks without active supervision from a human, then IoT objects for the home also fall within this category. In fact, it is sensors and actuators that make the object autonomous and, in some cases able to perform physically tangible tasks (such as opening a window, switching on the washing cycle for dishes). That is why, maybe in an attempt to be more comprehensive and lay out policies that could actually cover most of connected objects, the European Parliament decided to approve the Civil Law Rules of Robotics resolution[384], with a dedicated section on liability[385]. This section urged the Commission to create a legislative instrument, on the basis of Article 114 TFEU, concerning the civil liability rules of robots which should also include "[…] *legal questions related to the development and use of robotics and AI foreseeable in the next 10 to 15 years, combined with non-legislative instruments such as guidelines and codes of conduct as referred to in recommendations set out in the Annex*"[386]. The main takeaways from this section can be divided into groups.

The first group of considerations concerns the principles that a future civil liability scheme should have. Firstly, after a preamble on the need to ensure predictability and "directability" in the human-object relationship, the resolution declares the principle of full compensation for the damage to property that a robot might cause[387]. Secondly, the European Parliament (EP) asked the European Commission (EC) to consider whether a strict liability approach is better than risk management to underpin future legislation on the liability of robots. Thirdly, it argues that liability should be "[…] *proportional to the actual level of instructions given to the robot and its degree of autonomy, so that the greater a robot's learning capability or autonomy, and the longer a robot's training, the greater the responsibility of its trainer should be […]*"[388]. Finally, the EP advanced the

[381] Opinion 8/2014, 6-9.
[382] More on this in Chapters IV-V-VI.
[383] See Chapter II,
[384] European Parliament, *Civil Law Rules on Robotics European Parliament resolution (2015/2103(INL)*,Accessed 04 February 2022, http://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.pdf. Hereinafter Civil Law Rules of Robotics Resolution.
[385] Which will be dealt with in the next chapter.
[386] Paragraph 51, Civil Law Rules of Robotics Resolution.
[387] Paragraph 52, Civil Law Rules of Robotics Resolution.
[388] Paragraph 56, Civil Law Rules of Robotics Resolution.

hypotheses that for some kinds of robots (e.g., self-driving cars) the most efficient legal solution might consist of a mandatory insurance scheme[389].

The second group of suggestions consists more of a series of instructions to the EC contained in paragraph 59 and therefore has a more operative tone. Briefly, it requested the Commission to decide whether to set up: *i)* a mandatory insurance scheme for some kinds of robots or a *ii)* compensation fund that, if funded by the manufacturer, programmer and owner or user the result would be a *iii)* limited liability for each of those subjects. Alternatively or in addition to the previously suggested measures, the EP also urged the Commission , a) to decide whether to create a general fund for all smart autonomous robots, or to create a fund for each robot category and "[…] *whether a contribution should be paid as a one-off fee when placing the robot on the market or whether periodic contributions should be paid during the lifetime of the robot b) to create an individual registration number for robots in the EU and finally c)* ***to create a specific legal status for robots such as "electronic personality"***[390] *which could make sense with very autonomous robots*[…]". This last request was highly criticised because it allegedly favoured the deresponsibilisation of robot producers and manufacturers, which would not be in any case liable for damages. Given that drones were mentioned in the resolution, the exoneration of liability for damages (which include also erroneous murders) of their producers was met with concern, even though, in this context, liability was only connected to civil law[391]. In this resolution it is important to notice that the term "robots" was the one mentioned first, even before AI, which appeared to be employed as either a synonym or just a further and almost inevitable phenomenon.

Despite this first emphasis on robots, the Commission then decided to shift its focus from robots (and IoT) to AI in two communications[392]. This process started with the so-called soft law approach[393]. At the same time, there was a particular need to create a regulation after this initial soft-law approach. The first major step towards a legislative framework consisted in the creation of

[389] Paragraphs 57-58, Civil Law Rules of Robotics Resolution.
[390] Emphasis added.
[391] In further documents described infra, such as the Expert Group on Liability of AI and New Technologies, the argument for establishing an electronic personhood was abandoned not only on more ethical grounds but also on practical ones: at the moment it is always still possible to identify a human agent who directs the object. Expert Group on Liability and New Technologies, *Liability for Artificial Intelligence Report from the Expert Group on Liability and New Technologies-New Technologies Formation* European Commission, (Brussels:2019), 37-39.
[392] "COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Artificial Intelligence for Europe COM/2018/237 final," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN and "COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Coordinated Plan on Artificial Intelligence COM/2018/795 final," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:795:FIN.
[393] Guido Alpa, "Quale modello normativo europeo per l'intelligenza artificiale?," in *LA RESPONSABILITÀ CIVILE NELL'ERA DIGITALE (Atti della Summer school 2021)* Valentina V. Cuocci, Francesco Paolo Lops, Cinzia Motti (Bari: Cacucci editore, 2022),3-6.

a High Level Group on AI (AI-HLEG)[394] which firstly published a part of the Ethical guidelines on Trustworthy AI at the end of 2018, which was further edited and more structured at the beginning of 2019[395]. In this document, there is an emphasis on ethics and the need for this technology to comply with four general principles: respect for human autonomy, prevention of harm, fairness and explicability[396]. However, the trustworthiness that such technology should aim at does not only rely on ethics and a robust technology from a cybersecurity point of view, but also on the fact that there must be legal instruments and remedies that can actually help users have trust in the system. The part concerning legal remedies, however, is not addressed in this document, or, rather, is addressed from a different angle, by focusing more on the principles of accountability and reliability of AI systems[397].

For EU citizens it may seem that only the EU has tackled the challenges and opportunities presented by AI through guidelines. However, it is important to stress that in that particular period, not only was the EU trying to give ethical guidelines to AI, but there were also other international organisations, such as OECD or sector-led organisations such as the Association for Computer Machinery (ACM) trying to do the same[398]. Furthermore, individual countries such as France, the UK, China[399] and Italy[400] drafted their own digital strategies to develop AI, along with important tech companies, such as Google[401]. The US, instead, decided to implement an R&D strategy[402].

Of the legal remedies that could be applied to robots, the IoT and AI, it is an educated guess that civil liability rules will become (if not the only ones), one of the most important sets of legal remedies for future IoE. In fact, it appears that personal and criminal liability applied to these technologies is not an option (at least for now) given the reaction to robots' E-personality unleashed by the EP Civil Law Rules on Robotics resolution. In 2018, also as a consequence of the

[394] The AI-HLEG stopped working in 2021, but all its history and documents can be found here, AI Alliance, Accessed 31 January 2023, https://ec.europa.eu/futurium/en/european-ai-alliance/ai-hleg-steering-group-european-ai-alliance.html.
[395] AI-HLEG, *Ethics Guidelines for Trustworthy AI* (Brussels, 2019), https://doi.org/102759/346720.
[396] AI-HLEG, *Ethics Guidelines for Trustworthy AI* (Brussels, 2019), 8-12.
[397] AI-HLEG, *Ethics Guidelines for Trustworthy AI* (Brussels, 2019), 6.
[398] In particular, some studies included statistical research concerning the recurrent words in these guidelines. Transparency as a term appeared in 73/84 documents, whereas responsibility and accountability are not very well defined. Instead, privacy, though not clearly defined, is presented together with terms such as data security. See Anna Jobin, Marcello Ienca, and Effy Vayena, "Artificial Intelligence: the global landscape of ethics guidelines," *Nature Machine Intelligence* 1 9 (2019) : 395-397.
[399] Martin Ebers, Standardizing AI. The Case of the European Commission's Proposal for an Artificial Intelligence Act." In *The Cambridge Handbook of Artificial Intelligence. Global Perspectives on Law and Ethics*, Larry A. Dimatteo, Cristina Poncibò and Michel Cannarsa (Cambridge: Cambridge University Press, 2022), 324.
[400] Ministero dello Sviluppo Economico (MISE), *Proposte per Una Strategia italiana per l'intelligenza artificiale,"* MISE website, Accessed 31 January 2023, https://www.mise.gov.it/images/stories/documenti/Proposte_per_una_Strategia_italiana_AI.pdf.
[401] Anna Jobin, Marcello Ienca, and Effy Vayena, "Artificial Intelligence: the global landscape of ethics guidelines," *Nature Machine Intelligence* 1 9 (2019): 395-397.
[402] Martin Ebers, Standardizing AI. The Case of the European Commission's Proposal for an Artificial Intelligence Act." In *The Cambridge Handbook of Artificial Intelligence. Global Perspectives on Law and Ethics*, Larry A. Dimatteo, Cristina Poncibò and Michel Cannarsa (Cambridge: Cambridge University Press, 2022), 324.

beginning of the HLEG's work, the Commission started a process evaluating the ability of MS legal systems to face the changes brought forward by new technologies. That is why two *ad hoc* expert groups were created. The first is the Expert Group on Liability and New Technologies- New Technologies formation[403]. The second one, instead, focused more intensely on the EU product liability regime and how new technologies would impact it. This was already mentioned when introducing the PLD in this same chapter[404].

As far as the first Expert Group (EG) is concerned, it published a report at the end of 2019. In the report it was maintained that, at that moment in time, the liability systems of the MS were not providing sufficient warrantees to consumers[405]. The experts recognised the specific features of "[…] *complexity, opacity, openness, autonomy, predictability data-drivenness and vulnerability* […]" [406] which were not present in objects before and that were likely to impact on the liability regime of the MS in the near future. Among the main findings, it was considered that regimes of fault liability could actually be considered as fit to address the issue of liability of new technologies for non-high risk AI and other emerging technologies applications[407]. Instead strict liability regimes were considered the solution for dealing with high-risk AI-technologies in public places[408]. The reference to the Operator, a new subject in the liability framework for new technologies, was considered to be an innovative part of the EG report. First of all, it is defined as either front-end ("the person primarily deciding and benefitting from the use of the relevant technology") or back-end ("the person continuously defining the features of the relevant technology and providing essential and ongoing backend support) operator. The principle is that liability should lie with the operator who is more in control[409]. Operators as well as producers are also bearers of duties of care, such as: choosing the right system for the right tasks and skills, monitoring it and maintaining it[410]. According to the

[403] Expert Group on Liability of AI and new technologies portal, Accessed 31 January 2023, https://ec.europa.eu/transparency/expert-groups-register/screen/expertgroups/consult?do=groupDetail.groupDetail&groupID=3592

[404] "REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL AND THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE on the Application of the Council Directive on the approximation of the laws, regulations, and administrative provisions of the Member States concerning liability for defective products (85/374/EEC) COM(2018) 246 final," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0246&from=DE, 9

[405] Expert Group on Liability and New Technologies, *Liability for Artificial Intelligence Report from the Expert Group on Liability and New Technologies-New Technologies Formation* (European Commission: Brussels, 2019),32

[406] Expert Group on Liability and New Technologies, *Liability for Artificial Intelligence Report from the Expert Group on Liability and New Technologies-New Technologies Formation* (European Commission: Brussels, 2019),32

[407] Expert Group on Liability and New Technologies, *Liability for Artificial Intelligence Report from the Expert Group on Liability and New Technologies-New Technologies Formation* (European Commission: Brussels, 2019),40

[408]Expert Group on Liability and New Technologies, *Liability for Artificial Intelligence Report from the Expert Group on Liability and New Technologies-New Technologies Formation* (European Commission: Brussels, 2019),40.

[409] [11], Expert Group on Liability and New Technologies, *Liability for Artificial Intelligence Report from the Expert Group on Liability and New Technologies-New Technologies Formation* (European Commission: Brussels, 2019).

[410] [16] Expert Group on Liability and New Technologies, *Liability for Artificial Intelligence Report from the Expert Group on Liability and New Technologies-New Technologies Formation* (European Commission: Brussels, 2019).

report, producers instead would be responsible (irrespective of whether they also have operators' functions) of carefully designing, describing and marketing products, and effectively monitoring the same products after placing them in circulation[411].

The new concepts of "commercial and technological unit" and "damage to data" are particularly interesting as well as the suggestion of new principles on how to assess evidence. With regard to the meaning, technological unit is not clearly explained *per se* but it is described as "*a group of two or more people* [who] *cooperate on a contractual or similar basis*" [412] with, I assume, the objective of providing a unitary digital service or interconnected good. Therefore, it will often be a producer, an operator or groups made up of several of them. The EG does not fully explain what the origin of damage to data is but it explains that it can entail liability "[…]*(a) when it arises from a contract or (b) liability arises from interference with a property right in the medium on which the data was stored or with another interest protected as a property right under the applicable law; or c) the damage was caused by conduct infringing criminal law or other legally binding rules whose purpose is to avoid such damage; or (d) there was an intention to cause harm*.[…]"[413]. If these principles were to be applied, this would mean that the SDG and the DCDS could also be used as sources of the contract that is referenced in letter (a).

Most remarkably, a series of procedural principles were suggested in order to make it easier for EU citizens to have remedies against AI-created damages. Firstly, the producer is considered liable for defects in emerging digital technologies even when the defect appears after the product was placed in circulation (thus eliminating the development risk exception with specific reference to the PLD, but also the SDG and DCDS could be involved in relation to the obligation to supply updates)[414]. Another obligation connected to the design of the product is to choose a technology that is able to store data about the product's use and how the product operates in a way that also the consumer could understand the (so-called *logging by design* principle)[415].

For remedies, there are several principles that the EG agreed on. Although for tort liability the rule will still be that the victim has to prove damage, a causal link and the infringement of a duty of care (or the existence of a contract if the

[411] [17] Expert Group on Liability and New Technologies, *Liability for Artificial Intelligence Report from the Expert Group on Liability and New Technologies-New Technologies Formation* (European Commission: Brussels, 2019).
[412] [29] Expert Group on Liability and New Technologies, *Liability for Artificial Intelligence Report from the Expert Group on Liability and New Technologies-New Technologies Formation* (European Commission: Brussels, 2019).
[413] [32] Expert Group on Liability and New Technologies, *Liability for Artificial Intelligence Report from the Expert Group on Liability and New Technologies-New Technologies Formation* (European Commission: Brussels, 2019).
[414] [14] Expert Group on Liability and New Technologies, *Liability for Artificial Intelligence Report from the Expert Group on Liability and New Technologies-New Technologies Formation* (European Commission: Brussels, 2019).
[415] [20] Expert Group on Liability and New Technologies, *Liability for Artificial Intelligence Report from the Expert Group on Liability and New Technologies-New Technologies Formation* (European Commission: Brussels, 2019).

relationship is contractual) there is an exception: "*the burden of proving defect should be reversed if there are disproportionate difficulties or costs pertaining to establishing the relevant level of safety or proving that this level of safety has not been met*"[416]. A reversal of proof is however contemplated in two other cases: when the provision of logging by design is not present[417], and also *"where the damage is of a kind that safety rules were meant to avoid, failure to comply with such safety rules, including rules on cybersecurity, should lead to a reversal of the burden of proving (a) causation, and/or (b) fault, and/or (c) the existence of a defect.*"[418]

The EG did not only express its ideas on the liability of AI and new technologies. A study conducted by the European Parliament[419] (EP) instead considered that, even admitting how important the EG work was in terms of recognising the state of the art, it had some limits. In general, it was considered that the expression "AI and other emerging technologies" was too general and did not get the main differences among different AI applications and AI technologies. It was pointed out that the definition between high-risk and low-risk application based on the Learned Hand formula [420] did not make much sense outside the US legal system[421]. Moreover, the request of effective remedies and a same level of fairness for damages caused by AI compared with damages not caused by AI, was then followed by a preference for evidentiary rules over substantive ones[422]. Moreover, the relationship between the (improved) PLD and more specific regulations, such as safety ones was not clear[423]. However, both the EG and the EP study consider that it will be sensitive to increase the post-contractual duties, in particular the duty to update the objects both for the operator and the producer[424].

More or less at the same time in which both the EG and the EP studies were published, the IoT was distinctly present in one Commission working staff document. It concerned the safety and security of AI, IoT and Robots[425]. However, the working staff document contents more or less coincided with the

[416] [15] Expert Group on Liability and New Technologies, *Liability for Artificial Intelligence Report from the Expert Group on Liability and New Technologies-New Technologies Formation* (European Commission: Brussels, 2019).
[417] [22] Expert Group on Liability and New Technologies, *Liability for Artificial Intelligence Report from the Expert Group on Liability and New Technologies-New Technologies Formation* (European Commission: Brussels, 2019).
[418] [24] Expert Group on Liability and New Technologies, *Liability for Artificial Intelligence Report from the Expert Group on Liability and New Technologies-New Technologies Formation* (European Commission: Brussels, 2019).
[419] Andrea Bertolini for EPRS, *Artificial Intelligence and Civil Liability- Legal Affairs Report* (Brussels: European Parliament, 2020). Hereinafter, Bertolini EP Study (2020)
[420] It was the formula which calculated the probability for a tort to be compensated by including notions of damage, probability of damage and burden of precaution. More on this in Section 1.1. of Chapter V.
[421] Bertolini EP Study (2020),77.
[422] Bertolini EP Study (2020), 81-83.
[423] Bertolini EP study(2020):76.
[424] Bertolini EP study(2020:86-87.
[425] "REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL AND THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, COM(2020)64 final,"EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1593079180383&uri=CELEX%3A52020DC0064.

results of the EG study[426], hence the IoT was not dealt with really *per se* but always together with AI[427].

After that, the Commission published its digital strategy plans in early 2020 and, in particular, its white paper on Artificial Intelligence[428] and its data strategy[429]. However, there was no explicit mention of the IoT or its liability in any of them. The European Parliament asked the Commission directly in October 2020 to regulate the AI and its regime of civil liability [430]. Especially this last document is important for this work, as it and the Commission responded by publishing a draft proposal on the regulation of the AI (AI act, AIA) by April 2021[431]. However, the AIA proposal lacks the civil liability aspect that the European Parliament had requested in its resolution.

Before proceeding with the examination of the main features of the AIA and its application rules involving IoT objects (including the ones for the home), it is important to describe the content and main features of the second resolution of the EP on liability. This time, robots are not the technological term used the most, but AI is.

In 2020, the EP asked the Commission to create a regulation on the civil liability of AI, on the basis of Articles 114, 169 and 225 TFEU[432]. It is an interesting document as it summarises and selects a part of the findings that were gathered by the EP's previous resolution of 2017, the expert group on liability and new

[426] For instance the characteristics of connectivity, autonomy, complexity, openness, ospacity and (low) cybersecurity are mentioned on page 2 of the report and they are the same features on which the EG drafted its report. "REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL AND THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, COM(2020)64 final,"EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1593079180383&uri=CELEX%3A52020DC0064, 2.

[427] Also on page 2 of the same report, one can notice that the titles always unite AI and the IoT, for instance 1.2 and 1.3 always mention AI and the IoT together. For instance, title 1.2 is drafted as follows, "Characteristics of AI, IoT and Robotics Technologies". Subtitle 1.3 instead reads "Opportunities created by AU, IoT and Robotics." REPORT FROM THE COMMISSION TO THE EUROP PARLIAMENT, THE COUNCIL AND THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE Report on the Safety and Liability Implications of Artificial Intelligence, the Internet of Things and Robotics, COM(2020)64 final,"EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1593079180383&uri=CELEX%3A52020DC0064 ,2.

[428] "WHITE PAPER On Artificial Intelligence - A European approach to excellence and trust COM/2020/65 final," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0065.

[429] "COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A European strategy for data COM/2020/66 final," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066.

[430] "European Parliament Resolution 20 October 2020 P)_TA(2020=0276 Civil liability regime for artificial intelligence," EP, Accessed 31 January 2023, https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_EN.html#title1.

[431] "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS COM/2021/206 final," EUR-Lex, Accessed 31 January 2023 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

[432] "European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)) *OJ C 404, 6.10.2021, p. 107–128,*" EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020IP0276. EP Liability Resolution 2020.

technology findings and the studies that were required by the EP itself[433]. Unlike in the EP study, it is underlined how having a clear, efficient and most of all uniform liability system is essential to exploit all the advantages of AI and it appears that it advocates new ways to apply liability rules to AI applications[434]. One thing instead that the EP resolution borrows from the EG report is the choice of introducing software front-end and back-end operators as potentially liable subjects. Moreover, the input that there should be a division between high-risk and low-risk applications is from the EG, hence the different consequences in terms of liability. For instance, if a high-risk application is deployed in a public space, the kind of liability employed should be strict liability[435]. Also, one year before the AI regulation, it recommended listing the high-risk applications in a dedicated Annex[436] which is what actually happened (see below). Conversely, all non-high risk systems should instead be based on a fault liability system[437]. This general distinction does not really assess the main problem, which is that AI is a multi-dimensional phenomenon and that just because an application is considered less risky in general, it cannot cause potentially greater damage than high-risk AI applications [438].

Despite the fact it does not tackle private law liability, the AIA is a model that needs to be considered and studied, especially if high-risk IoT applications (such as healthcare IoT and industrial IoT objects) are assimilated to AI high-risk applications from a regulatory point of view. In fact, it seems unlikely that even high-risk IoT applications would receive an *ad hoc* regime at this point. The AIA definition of AI system[439] is narrower than the one given by the HLEG[440] group, by also including statistical methods through the connection to the relative Annex I. What is relevant is whether high, medium or low risk AI systems (algorithms or groups of algorithms) are used. Let us take as an example a monitoring vest that is useful for doctors to carry out remote visits with patients from their home. This is an IoT with medical functions *per se*, but through the hospital cloud, it also probably uses some of the types of algorithms that are listed in Annex I. The object as well as the algorithms that make it work from the cloud could be considered high-risk AI system applications. This evaluation has to take into account several other factors that could not be known *in abstracto*. If that is the case, however, meaning the IoT uses high-risk algorithms in a high-risk context, the AIA rules will apply to them even if these algorithms are a functioning part of an IoT object. In Chapter VI, it will be explained that with the "American Good AI Act" this would not be possible, as the definition excludes "*any common or*

[433] Bertolini EP study (2020)
[434] EP Liability Resolution 2020, 2
[435] EP Liability Resolution 2020. 14
[436] EP Liability Resolution 2020. 16
[437] EP Liability Resolution 2020. 20
[438] Andrea Bertolini and Francesca Episcopo, "The Expert Group's Report on Liability for Artificial Intelligence and Other Emerging Technologies: A critical assessment," *European Journal of Risk Regulation* 12,3 (2021): 644-659, https://dx.doi.org/10.1017/err.2021.30.
[439] See Chapter I, subsection 1.5.
[440] The AI-HLEG guidelines define AI as made of three components in order to be trustworthy: it needs to be lawful, ethical and robust, but does not define the technologies that need to respect these requirements. AI-HLEG guidelines, 5.

commercial object in which artificial intelligence is embedded," hence, the IoT[441]. It is too early to say which of the two regulatory approaches would prove more efficient.

As far as the rationale is concerned, the AIA, like the GDPR, should balance a fundamental rights protection function approach with a risk management one. However, the fundamental rights element is sometimes less developed than the risk management one[442]. It is interesting to analyse some of risk-based approach applications that are not at all new, but adapted to this new context. Most notably, we can find compliance duties according to the degree of risk of the AI system[443], codes of conduct[444] , the use of Notified Bodies[445],and the use of harmonised standards[446].

The other important feature of the proposal is that the AI follows a trend started under the New Approach and pursued under the New Legislative Framework: risk management at regulatory level is handled with tools that mix private and administrative (public) functions and rationales. Therefore, it blurs the boundaries between the concepts of accountability and liability. In the AIA the codes of conducts are non-mandatory, but they are suggested means for proving compliance, and, for riskier applications, the system of Notified Bodies (NB) which was firstly developed for the MDD now MDR, is adapted to AI system evaluation and application. It must be recalled that in the exercise of their subsidiarity power, the MS can decide whether to suggest to the Commission *a)* private *b)* public *c)* public-private entities as NB.

Another important feature is that the AIA is similar to the DGA and the GDPR in creating a coordination board, which would mix and represent the instances coming from MS and the institutions: the European Artificial Intelligence Board[447]. This responds to a governance issue, but also to a "constitutional" one as competences in the EU can be either unique to the EU or MS or shared[448]. There might be an issue of efficiency, especially if communication and coordination among members takes time. In this respect, a working and functioning example of this kind of synergy between competent national and EU authorities is the EDPB.

It is true that at the time of speaking, the majority of IoT objects for the home have neither great automatisation skills nor interactive skills. However, progress

[441] See Chapter VI, subsection 1.2.
[442]This last critique came both by the dedicated EP committee which had to evaluate the proposal and by the Social and Economic Committee which suggested the EU Commission to take a bolder stance in forbidding AI powered facial recognition systems. Social and Economic Committee, "Opinion of the Social and Economic Committee on the EC proposal on the regulation of AI, COM 205/2021 final," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021AE2456.
[443] For instance, transparency and human oversight ones, Articles 9-15 and 52 AIA and post market surveillance ones: 61-62 AIA.
[444] Articles 69-72 AIA.
[445] Chapter IV AIA.
[446] Chapter V AIA.
[447] 56-58 AIA.
[448] The constitutional aspects of liability will be dealt with in chapter IV, section 2.

in computational power and software (AI) and new technologies such as DLTs, Edge Computer and Blockchain are not only merging and pushing forward the evolution of the IoT as objects, through the process of technical convergence, but are increasing the connection between people and (domestic) IoT, thus paving the way to the creation of an Internet of Everything (IoE) as defined in the methodology chapter[449]. This is accentuated by the further development of wearable devices and mixed function health-consumer IoT, which will be mostly used in the home.

The proposed AIA will surely be a model for those applications of IoT objects that for their complexity and reliance on the kind of algorithms indicated in Annex I of the AIA could be considered high-risk AI systems at large. However, unless there are *ad hoc* AI liability regimes drafted in the meantime, the only EU private law liability framework for new technology at the moment of writing is the PLD, which is currently undergoing an updating process. This is because the division into high- and low-risk AI systems is indeed relative in terms of possibility of creating damages: even a smart-coffee maker could set fire to a home and create huge property damages[450]. This means that even an object which is considered low risk could actually create serious damages on its own or because of the characteristics of the person using it (e.g., a baby, a person with a disability or a senior person) especially in a domestic environment. The case in which a kid was ordered by Alexa to put a metal coin in an electric plug demonstrates the previous argument[451].

In order to reply to the research question of Chapter I on methodology, I conclude that there is indeed the need for new rules for domestic IoT objects and that it is possible to do that by updating the rules of the PLD, as it is the EU private law document which has not been formally updated yet at the moment of writing[452]. That is why the next chapter will be focused on showing how product liability differs from other kinds of liability at the level of EU harmonization[453]. The PLD will then be examined in depth to understand whether its history can give us insights for its update[454] and then there will be a final comparison with the US product liability model[455]

[449] Chapter I.
[450] This was actually what happened in the *Fennia* case, in which a coffee maker (probably a smart coffee maker) created a fire in a private home in Finland. See in Chapter V, under section 3, Future Article 3 PLD.
[451] BBC News Tech, "Alexa tells a 10-year-old girl to touch live plug with penny," December 28, 2021, https://www.bbc.com/news/technology-59810383.
[452] Meaning 31 August 2022.
[453] Chapter IV.
[454] Chapter V.
[455] Chapter VI.

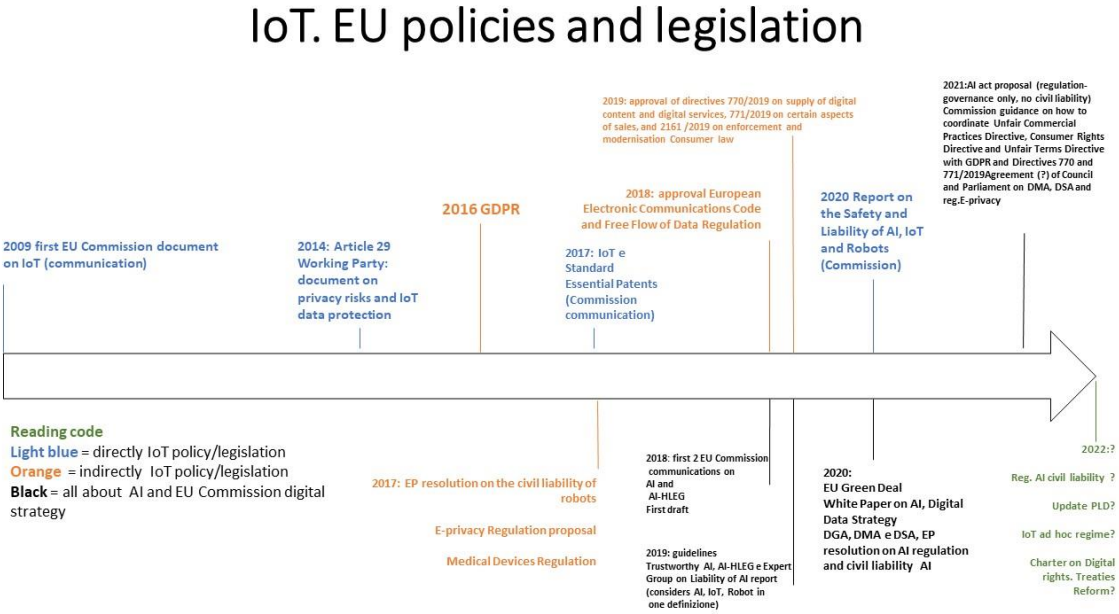

Figure 1 Timeline concerning IoT policy

Chapter IV: Liability in the EU and in the smart home

Chapter IV: Liability in the EU and in the smart home 96
1. Liability and the smart home: past rationales and new meanings96
1.1. The "traditional" functions and features of private law liability 97
1.1.1. The general functions of liability..... 97
1.1.2. The different features of EU private law liability and their degree of harmonization 98
I. Extra-contractual/Tort Liability 99
II. Strict Liability- Objective and quasi objective-strict liability..... 104
III. Contractual liability..... 106
IV. Pre-contractual liability..... 109
1.2. Liability: between risk and innovation 110
1.3. Liability: a balance between different actors 111
1.4. Liability: an enhancer of Trust in IoT technology for the home 115
1.5. Liability in a home that changes: how perceptions of the home environment have changed and their impact on liability..... 116
2. Liability in EU private law and the smart home 122
2.1. The EU criteria for competence: the principle of conferral and the principle of subsidiarity..... 122
2.2. Is Article 114 TFEU (harmonization) and the single market clause enough to establish liability for new technologies in general?..... 125
2.3. The Charter for Digital Rights and a progressive path towards a more Constitutional oriented legal integration of new technologies..... 130
3. Product Liability for the home IoT: which possible constitutional scenarios? 132

1. Liability and the smart home: past rationales and new meanings

This chapter has one main function: to transition from the state of the art to the core part of the thesis. In order to do that, the chapter has two main content parts. The first one is dedicated to the functions of liability. After detailing the state of the process of liability harmonization in the EU and the rationales that the different kinds of private liability have (1.1), I will argue that liability must not only be seen as connected with litigation, but also with the processes that create innovative technologies (1.2), allocate risk (1.3), and which create trust in consumers-users-citizens (1.4). Finally, there will also be a description of how the home has changed abruptly since 2020 and which impacts there might be on home-technology and related liability rules (1.5). If the social and economic function of liability for the connected smart home object is demonstrated, then it is time to start again from the results of Chapter III to understand whether the

legal basis for a smart home IoT objects liability system is granted by the actual system of the EU Treaties (2). I will argue that we are all currently living in an intermediate phase where the basis for the internal market is likely to be no longer sufficient for the needs of the Digital Single Market, which since its beginning has paired fundamental rights and regulatory approaches. Moreover, I believe that this different origin process of the Digital Single Market is also likely to influence the creation of a new PLD(3).

1.1. The "traditional" functions and features of private law liability

In this subparagraph, I will try first to analyse the general functions of private liability law, intended in a traditional legal sense. As for traditional, I intend to focus mostly on continental law theory, and in particular, on the developments that codification brought into EU Member States from the time of the first private law codifications. Therefore, I will try to describe the main functions of each kind of private law liability in a concise manner. I have decided to use these subparagraphs as entry level tools for concepts that I will deal with in detail in Chapters V and VI. While doing that, I will try to describe the main features of each kind of private law liability and to the degree to which the EU in Europe has played a role in harmonising the various, pre-existing legal models. This will be helpful in order to outline how and why these forms of liability are impacted by technology.

1.1.1. The general functions of liability

Generally, liability can be defined as the sanction for not abiding by a legal duty[456]. Despite that, in continental law theory, the legal scholars tend to agree on assigning a compensatory function to liability in addition to a preventive/deterrence function and a distribution of losses/allocation of risks one[457]. With regard to the compensatory function, its objective is to recreate the system that was pre-existent to the damage which happened to one of the parties involved, an objective that finds its roots in scholastic philosophy[458]. The private liability compensatory function is also confirmed by the fact that, in most EU codifications, the rules concerning the quantification of damages are almost the same, despite the fact liability might arise from a breach of a legal duty contained

[456] Manuela Rinaldi, "RESPONSABILITÀ OGGETTIVA IN GENERALE," In *Trattati Giuridici Omnia-La Responsabilità Civile, vol III*, Paolo Cendon (Torino: Utet Giuridica, 2020, 2nd ed.), 3539.
[457] In particular, the Italian legal scholars have used extra-contractual (tort) liability as the starting point for more general reflections about the functions of liability in general within a specific legal system and their relationship with society in a similar way as in the US, where the discussion about the functions of tort law started with the increase of legal actions specifically targeted to obtain remedies in tort. See among many: Mauro Bussani, *L'Illecito Civile* (Napoli: Edizioni Scientifiche Italiane, 2020),113-160; Pietro Trimarchi, *La Responsabilità Civile: Atti Illeciti, Rischio, Danno* (Milano: Giuffrè Francis Lefebre, 2019), 3-21; Stefano Rodotà *Il Problema della Responsabilità Civile* (Milano: Giuffrè, 1964), 16-25.
[458] Mauro Bussani, "LE FUNZIONI DELLE FUNZIONI DELLA RESPONSABILITÀ CIVILE," *Rivista di diritto civile* 2 (2022):273.

in a contract (contractual liability), or by a fault/negligence-based damage caused to another subject with whom there was no previous relationship (hereinafter extra-contractual/ tort liability)[459]. However, common law countries such as the US tend to associate liability more often with morality and, sometimes, with overarching concepts of fairness[460], even though these concepts have been challenged by a more economy-focused approach[461]. Nevertheless, in common law, liability does not only possess a compensatory and preventative function, but its connected remedies also still reflect a punitive function[462]. That is why the damages that are attributed to the plaintiff are generally called punitive damages[463]. This function was not admitted for most European substantial and procedural continental civil laws (with the exception of common law countries, which still apply them but not with the same frequency as the US[464]). Nevertheless, some EU judgments, such as *Von Colson and Kamann* and also the Rome II regulation might be interpreted as leading to a partial acceptance of punitive damages, provided they are not excessive[465]. It is worth mentioning that Italy in particular, with two successive Court of Cassation judgments, admitted the partial applicability of punitive damages as a form of execution of US judgments[466].

1.1.2. The different features of EU private law liability and their degree of harmonization

[459] This is the case for the Italian legal system, where the only difference in the quantification of damages is the lack of reference in Article 1225 Italian Civil Code (ICC) regarding extra-contractual (tort) liability. This omission makes it impossible to obtain unforeseeable damages caused by fault in tort. This provision originated from the French Code Civil, which maintained it in Article 1231-3 of the French Civil Code (FCC, previously Article 1150 FCC), even after the reform of Obligations law in 2016. Mauro Bussani, *L'Illecito Civile* (Napoli: Edizioni Scientifiche Italiane, 2020),

[460] George P. Fletcher, "Fairness and Utility in Tort Theory," *Harvard Law Review* 85,3 (1972) :550.

[461] Richard A. Posner, "The Concept of Corrective Justice in Recent Theories of Tort Law," *The Journal of Legal Studies* 10,1(1981): 187.

[462] Lemley and Casey argue that these motivations can also be inferred by analysing the different kinds of remedies available in the American system. They infer these functions from the analysis of the different remedies available. "[…C]*ompensatory remedies tend to address the wrongs suffered by an individual through monetary transfers between plaintiff and defendant, compensating the plaintiff for the injury suffered". Whilst "preventative remedies seek to discourage or literally undo harm* […] *through the payment of damages, restitutions or specific performances and finally there are also equitable restitutionary remedies (such as unjust enrichment) whose objective is … to make the defendant whole so that he is no better off than he would have been*." Mark Lemley and Bryan Casey, "Remedies for Robots," *The University of Chicago Law Review* 86(2018):1343-1344.

[463] They are defined *"…an additional sum over and above the compensation of the plaintiff for the harm suffered, which are awarded for the purpose of punishing the defendant, of admonishing the defendant not to do it again and of deterring others not to follow the defendant's example" Despite the fact they originated to publish abuses of power in George III England, they became quite common especially in tort cases, although their use was and still is quite debated among Common Law scholars* John W. Wade, et al., *Prosser, Wade and Schwartz' Torts* 9th ed (New York: University Casebook series 1994) 531, Jason Taliadoros, "The Roots of Punitive Damages at Common Law: A longer History," *Cleveland State Law Review* 64,2 (2016) 251-302.

[464] Helmut Koziol, "Punitive Damages- A European Perspective," *Lousiana Law Review* 6,3(2008): 741-764.

[465] Koziol Ibid. 748-751.

[466] Judgment n.7613, 15th April 2015, and Judgment n.16601, July 15th 2017.

This subsection's function is to provide a brief yet exact summary of the level of harmonization progress in EU countries' liability systems, with reference to extra-contractual/tort, contractual, pre-contractual and strict liability. This will be preliminary to the analysis of Article 114 TFEU in the second part of the chapter as a possible legal basis for the updated EU PLD, and in particular, the conclusion of this subsection is that strict liability, which is the model of liability of the current PLD, might be the most harmonised form of liability in the EU.

I. Extra-contractual/Tort liability

Tort law could be considered as a social legal tool that answers best the "[…] *aim to settle societal conflicts in the event of disruptions of social harmony* […]"[467]. In continental law tradition, the *fil rouge* connecting all the tort systems is the absence of a contract at the origin of the one party's obligation towards another. There are several models but maybe the best known are the French and the German ones, as they are antithetical. The French system is based on an extremely general clause which can cover several situations. The structure and scope of the former Article 1382 have not been changed by the new Article 1240 of the French Civil Code (FCC), which substituted the former during the reform of the Obligations in 2016. They both protect subjective rights and legitimate interests[468]. Moreover, unlike in Italy or Germany, French legal scholars have never felt the need to interrogate themselves on the actual breadth of protection offered by tort law[469]. In fact, whatever was not connected to the contract was immediately considered as part of extra-contractual liability, pre-contractual liability included. The opposite model, instead, follows the German civil code (Bürgerliches Gesetzbuch, BGB). To be applicable, the provision on extra-contractual liability (§823[470]) requires four kinds of requirements to be satisfied cumulatively. The first one is a violation of selected rights and interests, such as life, body, health, freedom, property or any other right[471]; the second one is that the violation must be unlawful[472]; the third one is that the violation must also be either negligent or intentional[473]; and the final requirement is that there must be a proof of causal link between the defendant's act or omission and the damage endured by the plaintiff[474]. In general, extra-contractual or tort liability in

[467] Despite the focus of this thesis is on continental law models of tort liability, it is important to remember that in many countries of the world there are official (State) and unofficial (non-State) tort law remedies. See Mauro Bussani and Marta Infantino, "The Many Cultures of Tort Liability," in *Comparative Tort Law. Global Perspectives*, Mauro Bussani, Anthony J. Sebok (Cheltenham: Edward Elgar, 2021),13-16.
[468] Walter van Gerven, Jeremy Lever and Pierre Larouche, *Cases Materials and Text on National, Supranational and International TORT LAW* (Oxford and Portland, Oregon: Hart, 2000),57.
[469] Walter van Gerven, Jeremy Lever and Pierre Larouche, *Cases Materials and Text on National, Supranational and International TORT LAW* (Oxford and Portland, Oregon: Hart, 2000),57.
[470] §823 is still the main article concerning extra-contractual law in Germany, unlike in France, even after the *Schuldrechtsmodernisierung*, the Reform of the Law of Obligations of 2001.
[471] Basil. S. Markesinis (Sir), *The German Law of Obligations. Volume II. The Law of Torts: A Comparative Introduction* (Oxford: Clarendon Press, 1997), 35.
[472] Basil. S. Markesinis (Sir), *The German Law of Obligations. Volume II. The Law of Torts: A Comparative Introduction* (Oxford: Clarendon Press, 1997), 35.
[473] Basil. S. Markesinis (Sir), *The German Law of Obligations. Volume II. The Law of Torts: A Comparative Introduction* (Oxford: Clarendon Press, 1997), 35.
[474] Basil. S. Markesinis (Sir), *The German Law of Obligations. Volume II. The Law of Torts: A Comparative Introduction* (Oxford: Clarendon Press, 1997), 35.

continental law is the plaintiff's duty to prove. Hence, generally, the plaintiff must prove the fault in the defendant's action or omission and the causation link connecting the damage to the action or omission[475]. Generally, the kinds of damages that can be recovered are both of a material and immaterial nature, but they are very differently evaluated in the EU. Specifically, for the latter ones, their assessment can be particularly problematic, especially when it comes to pure pecuniary loss[476] or moral damage, which *per se* is immaterial but can have tangible consequences on the health and life of the plaintiff. Moreover, there are still relevant differences as far as how the counts of damage will be indemnified or how favourably the national jurisdictions can compensate the plaintiffs according to the specific kind of loss consequent to the damage[477].

In the EU, as far as harmonization goes, extra-contractual/tort liability has been the one that has had the lowest level of harmonization, if we exclude from the analysis other specific kinds of liability, such as the strict liability models which instead have been harmonised by the PLD (see more infra)[478]. With regard to the EU institutions' liability, the Treaty of Lisbon makes it possible for EU institutions to be liable in general, also including tort liability in Article 340(2) TFEU. As far as a legal scholarship-inspired harmonization of European Tort law is concerned, it is important to cite the work of the European Group on Tort Law, which drafted the Principles of European Tort Law in 2005[479]. These principles are divided into ten general chapters (e.g., basic norm, damage and causal link)[480] and they were devised as a possible input for national and European legislators for an update or substitution of tort code rules[481]. In order to do that, the group did not take into account the most shared and known rules at a European level, but tried to find the best one to solve the problems which were specific to each element of extra-contractual liability, without considering the context in which the same rule was created[482].

Despite the current scenario, extra-contractual liability could play a significant role in technology cases: the Expert Group report on liability and new

---

[475] Ernst Karner, Bernard A. Koch and Mark Geistfield, *Comparative Law Study on Civil Liability for Artificial Intelligence* (Luxembourg: European Commission, 2021),22, https://dx.doi.org/10.2838/77360.
[476] Ernst Karner, Bernard A. Koch and Mark Geistfield, *Comparative Law Study on Civil Liability for Artificial Intelligence* (Luxembourg: European Commission, 2021),22.
[477] Ernst Karner, Bernard A. Koch and Mark Geistfield, *Comparative Law Study on Civil Liability for Artificial Intelligence* (Luxembourg: European Commission, 2021),22.
[478] Also, the Environment Liability Directive and the Motor Vehicle Insurance are both attempts at harmonising EU tort law. However, both these subjects, despite their interesting concepts and application mechanism, are beyond the scope of this research. See "Directive 2004/35/CE of the European Parliament and of the Council of 21 April 2004 on environmental liability with regard to the prevention and remedying of environmental damage. *OJ L 143,* 30.4.2004, p. 56–75,*"* EURLEX, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32004L0035. "Directive 2009/103/EC of the European Parliament and of the Council of 16 September 2009 relating to civil liability insurance in respect of the use of motor vehicles, and the enforcement of the obligation to insure against such liability (Codified version) (Text with EEA relevance) OJ L 263, 7.10.2009, p. 11–31," EURLEX, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32009L0103.
[479] Mauro Bussani, *L'Illecito Civile* (Napoli: Edizioni Scientifiche Italiane, 2020), 853-854.
[480] "European Principles of Tort Law," European Group on Tort Law, Accessed 31 January 2023, http://www.egtl.org/PETLEnglish.html.
[481] Mauro Bussani, *L'Illecito Civile* (Napoli: Edizioni Scientifiche Italiane, 2020), 853-854.
[482] Mauro Bussani, *L'Illecito Civile* (Napoli: Edizioni Scientifiche Italiane, 2020), 853-854.

technologies envisages fault liability, hence extra-contractual liability, as the default rule for all the low-risk technology applications (which in this case should be applicable to IoT domestic objects too), without excluding, whenever possible, that national systems can cumulate several kinds of liability[483]. Nevertheless, it has to be kept in mind that the *cumulus* of different liability actions is not always possible in Europe[484]. However, there are already concerns that the traditional tort law systems of the MS might not be fit to address the new challenges caused by AI systems and new technologies[485]. Among the main issues discussed, there is the fact that the damages that some jurisdictions might be reluctant to recognise and compensate (such as moral damage or pure pecuniary loss), will quickly become more relevant in the future; or, otherwise, that the proof of causation might be hindered by how sophisticated technology is. For instance, if a domestic IoT object is connected to the cloud, some form of Machine Learning (ML) algorithmic techniques could be applied to the data sent from the object. If the ML algorithm is a so-called black box one (meaning that the external observer can understand what the input and the output are, but nothing in between), then liability issues are going to be more complex. Let us imagine that a physical or property damage happens in the home, and there is the possibility that this ML algorithm gave the wrong reaction input to the initial object's input, which subsequently caused the damage. There is almost no possibility that even the developer can understand why the algorithm behaved in an incongruous way[486]. Hence the proof of causation, that is generally the plaintiff's task, becomes increasingly difficult. The Expert Group on AI and new technologies tried to address the issue. More than on substantive laws, the suggestions concerned procedural tools instead, which could include a logging by design option, which, if not implemented by the producer, could entail an alleviation of causation proof for the plaintiff[487].

Moreover, national tort liability regimes could play a bigger role whenever the liability for a defective standard is concerned. This is because standards are both enablers of technological development and, at the same time, represent the consensus of precise groups of stakeholders on what it takes for a product to be considered state of the art[488]. As already introduced in Chapter II, the relevance of standards for domestic IoT objects is crucial from a technological point of view. In facts, both the proposed regulation on Artificial Intelligence (AI act) and the Data Act repeatedly mention standards throughout their texts as a means through

[483] Expert Group on Liability and New Technologies-New Technologies Formation" (Luxembourg: European Commission, 2019):18.
[484] Ernst Karner, Bernard A. Koch and Mark Geistfield, *Comparative Law Study on Civil Liability for Artificial Intelligence* (Luxembourg: European Commission, 2021),20-21.
[485] Ernst Karner, Bernard A. Koch and Mark Geistfield, *Comparative Law Study on Civil Liability for Artificial Intelligence* (Luxembourg: European Commission, 2021),9.
[486] Cynthia Rudin and Joanna Radin, "Why Are We Using Black Box Models in AI When We Don't Need To? A lesson From an Explainable AI Competition," *Harvard Data Science Review* 1,2 (2019) https://dx.doi.org/10.1162/99608f92.5a8a3a3d.
[487] Points from [20]-[26]. Expert Group on Liability of AI and New Technologies "Liability for Artificial Intelligence Report from the Expert Group on Liability and New Technologies-New Technologies Formation" (Brussels: European Commission, 2019):7-8.
[488] Francesca Gennari, "Liability for IoT Standards in the EU. And yet it moves?," *Robotics & AI Law Society (RAILS) blog*, Accessed 31 January 2023 https://blog.ai-laws.org/liability-for-iot-standards-in-the-eu-and-yet-it-moves/.

which governance can be exercised and EU businesses can invest in these technologies. Apart from the democratic problems that the over-reliance on standards entails[489], as far as liability is concerned, the EU does not have an explicit strategy regarding which kind of liability is applicable to these IoT standards, if they cause damage. As far as the EU is concerned just two sources of IoT standards can be relevant: international and European harmonised standards.

At the international level, there are international standard setting/developing organisations, which develop and set standards, open or private, for IoT in various fields (connectivity, data privacy, the cloud)[490]. The standards they develop/set are generally not binding, unless they are incorporated in a national or European harmonised standard. However, most of these SDOs (such as IEEE and ITU) are considered leaders in the field and define the state of the art as far as technology is concerned. It is not clear what happens if an IoT manufacturer decides to use a standard and subsequently gets sued because that standard generated damage. At the moment, as already introduced in Chapter II, most EU countries might rely just on tort liability rules, but this would entail the same problems for the plaintiffs - as mentioned above- because of the difficult task of proving causation and the entity and compensability of damage, especially when the latter is not a tangible one. With regard to how to address the plaintiffs' hurdles, there might be differences not only between common law and continental law jurisdictions but also within the same continental law family in addressing this same issue [491]. Supposedly, France and Italy might use two different tools connected to contractual liability in order to facilitate the recovery of damages. French judges could allow the use of an *action directe* (recovery action)[492] and Italian judges the contractual theories based on the fact that the SDO has a duty, socially, to create safe standards, even when there is no contract because of the *contatto sociale qualificato* (qualified social contact)[493] with the consumer or the manufacturer. Germany,

[489] Martin Ebers, "Standardizing AI. The Case of the European Commission's Proposal for an Artificial Intelligence Act," in *The Cambridge Handbook of Artificial Intelligence. Global Perspectives on Law and Ethics*, Larry A. Dimatteo, Cristina Poncibò and Michel Cannarsa (Cambridge: Cambridge University Press, 2022), 332-333, 340-342. Martin Ebers, "Standardizing Artificial Intelligence. A Critical Assessment of the European Commission's Proposal for an Artificial Intelligence Act," *Robotics & AI Law Society (RAILS) blog*, Accessed 31 January 2023, https://blog.ai-laws.org/standardizing-artificial-intelligence/.

[490] Francesca Gennari, "Liability for IoT Standards in the EU. And yet it moves?," *Robotics & AI Law Society (RAILS) blog*, Accessed 31 January 2023, https://blog.ai-laws.org/liability-for-iot-standards-in-the-eu-and-yet-it-moves/.

[491] Francesca Gennari, "Liability for IoT Standards in the EU. And yet it moves?," *Robotics & AI Law Society (RAILS) blog*, Accessed 31 January 2023, https://blog.ai-laws.org/liability-for-iot-standards-in-the-eu-and-yet-it-moves/. Niamh Gleeson and Ian Walden, "Cloud computing, standards and the law," In *Cloud Computing Law*, Christopher Millard (Oxford: Oxford University Press, 2021, 2nd ed.), 501-524, https://doi.org/10.1093/oso/9780198716662.003.0015.

[492] Cédric Hélaine, "De la bonne utilisation de la garantie des vices cachés dans une chaîne de contrats," *Dalloz Actualité* (06 July 2022) 6-8; Matthieu Poumarède and Philippe le Toruneau "Chapitre 6312- Domaine de la responsabilité," In *Droit de la Responsabilité et des contrats*, Philippe le Tourneau (Dalloz; Paris, 2021-2022,12 th ed.), 2576-2586; Olivier Barret and Philippe Brun, "Vente: effets- Garantie contre les vices cachés," *Répertoire Dalloz* (2018):§587-592.

[493] This qualified social contact derives from the fact that one of the parties is in the position to inspire reliance and trustworthiness in the other. The evolution of *contatto sociale qualificato* and *obblighi di protezione* (duties of protection) has been extensively studied and schematised by Italian legal scholar Vincenzo Castronovo. See Vincenzo Castronovo, *La responsabilità civile* (Milano: Giuffrè, 2018).

instead, could still deny the application of a duty of protection by negligent certifying bodies to patients if claimants rely on contractual liability and not tort liability[494].

Harmonised standards are EU products of the New Legislative Framework[495]. According to this governance process, the Commission can give instructions to some European SDOs (such as ETSI, CEN, CENELEC) to develop specific standards which will need to follow the Commission's abstract indications, as set in Regulation EU/2012/1025[496]. Once the standard is published in the Official Journal, the CJEU has competence over it, as interpreted by the 2014 judgment *James Elliott Construction* C-613/14[497]. In any case, Article 340 TFEU[498] would help in holding the EU institutions accountable. It is noteworthy that in Article 29(4) of the proposed Data Act, the Commission can request the creation of harmonised standards in relation to specific types of data processing services. If a harmonised standard caused damage, would the Commission be liable? If so, it would also be problematic to assess the grounds on which an EU citizen could sue. As far as individual locus standing, the CJEU case law has always been restrictive, as in the *Plaumann case C-25/62*[499], hence it would be safer to rely on a preliminary reference procedure following Article 267 TFEU[500].

The most likely reaction is that even European SDOs might take out civil liability insurance, as the Notified Bodies must do[501]. Hopefully, there is an

[494] Specifically, this happened in Germany even recently, in the aftermath of the PIP scandal (defective breast prostheses). German judges, although they admitted the negligence of the certifying body, stated that liability needed to be proved through the rules of tort liability, hence by using §823. Francesca Gennari, "Liability for IoT Standards in the EU. And yet it moves?," *Robotics & AI Law Society (RAILS) blog*, Accessed 31 January 2023 https://blog.ai-laws.org/liability-for-iot-standards-in-the-eu-and-yet-it-moves/.

[495] European Commission, "New Legislative Framework," *European Commission*, Accessed 31 January 2023, https://ec.europa.eu/growth/single-market/goods/new-legislative-framework_es.

[496] "Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council Text with EEA relevance *OJ L 316, 14.11.2012, p. 12–33"* EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32012R1025. Francesca Gennari, "Liability for IoT Standards in the EU. And yet it moves?," *Robotics & AI Law Society (RAILS) blog*, Accessed 31 January 2023 https://blog.ai-laws.org/liability-for-iot-standards-in-the-eu-and-yet-it-moves/.

[497] "James Elliott Construction Limited v Irish Asphalt Limited, Case C-613/14," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62014CJ0613. Hereinafter *James Elliott Construction*. Francesca Gennari, "Liability for IoT Standards in the EU. And yet it moves?," *Robotics & AI Law Society (RAILS) blog*, Accessed 31 January 2023 https://blog.ai-laws.org/liability-for-iot-standards-in-the-eu-and-yet-it-moves/.

[498] Article 340 TFEU.

[499] "Plaumann & Co. v Commission of the European Economic Communities, Case C-25-62," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A61962CJ0025, hereinafter *Plaumann*. Francesca Gennari, "Liability for IoT Standards in the EU. And yet it moves?," *Robotics & AI Law Society (RAILS) blog*, Accessed 31 January 2023 https://blog.ai-laws.org/liability-for-iot-standards-in-the-eu-and-yet-it-moves/.

[500] Article 267 TFEU.

[501] Annex VII 1.4, 1-2."Medical Device Regulation (MDR) Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Text with EEA relevance.) *OJ L 117, 5.5.2017, p. 1–175,"* EUR-Lex,

ongoing and incremental harmonization of IoT standards remedies. Whether this actually is an indirect and, perhaps, almost casual consequence of the proposed Data Act, is yet to be seen.

II. Strict Liability- Objective and quasi objective-strict liability

As far as strict or objective liability (I will use the two as synonyms when I refer to the EU context), the most relevant element is that there is no need for the plaintiff to prove either fault or negligence. Moreover, this kind of liability can depend on the position of control the defendant has on the thing, animal or person that caused the damage. For this reason, it is also referred as *responsabilité sans faute,* or *objektive Haftnung*[502]. Sometimes, however, civil codes provide rebuttable presumptions even in the case of strict liability.

Historically, this form of liability emerged at the end of the 19th century in industrialised countries due to the emergence of a new "objectification" and the increasing "de-subjectification" that characterised the final product of the activity[503] that can cause damage[504]. This kind of liability originated first in industrialised states, such as the ones in North America and in Continental Europe. From the 2000s, product liability, which is generally connected to the strict liability family, was also already a global phenomenon[505]. Another reason why strict liability developed was to identify, control and prevent new risks[506]. This also explains why a synonym of strict liability in Germany is risk liability (*Gefährdungshaftung*)[507]. Finally, the third reason why this form of liability developed is that despite technology perhaps exposing people to new forms of risk, the benefits for society are still considered to be higher than the eventual costs and damages for the individual[508]. As a consequence, managing risks

---

Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R0745. Hereinafter MDR. Francesca Gennari, "Liability for IoT Standards in the EU. And yet it moves?," *Robotics & AI Law Society (RAILS) blog*, Accessed 31 January 2023 https://blog.ai-laws.org/liability-for-iot-standards-in-the-eu-and-yet-it-moves/.

[502] Cees Van Dam, "Strict Liability," In *European Tort Law*, Cees Van Dam (Oxford: Oxford University Press), 297.

[503] Antonino Fazio, "IL NESSO CAUSALE NELLA RESPONSABILITÀ OGGETTIVA E SEMI OGGETTIVA," In *Trattati Giuridici Omnia-La Responsabilità Civile, vol III*, Paolo Cendon (Torino: Utet Giuridica, 2020, 2nd ed.) 3533.

[504] Antonino Fazio, "IL NESSO CAUSALE NELLA RESPONSABILITÀ OGGETTIVA E SEMI OGGETTIVA," in *Trattati Giuridici Omnia-La Responsabilità Civile, vol III ,* Paolo Cendon (Torino: Utet Giuridica, 2020, 2nd ed.), 3533. Mathias Reimann, "Liability for Defective Products at the Beginning of the Twenty-First Century: Emergence of a Worldwide Standard ?," *The American Journal of Comparative Law* 51,4(2003) 758.

[505] Mathias Reimann, "Liability for Defective Products at the Beginning of the Twenty-First Century : Emergence of a Worldwide Standard ?," *The American Journal of Comparative Law* 51,4(2003) 758.

[506] Guido Calabresi and A. Douglas Melamed, "Property Rules, Liability Rules, and Inalienability: One View of the Cathedral," *Harvard Law Review* 85,6(1972):1089-1128.

[507] Cees Van Dam, "Strict Liability," In *European Tort Law*, Cees Van Dam (Oxford: Oxford University Press,2013), 297-306.

[508] Antonino Fazio, "IL NESSO CAUSALE NELLA RESPONSABILITÀ OGGETTIVA E SEMI OGGETTIVA In *Trattati Giuridici Omnia-La Responsabilità Civile, vol III,* Paolo Cendon *(*Torino: Utet Giuridica, 2020, 2nd ed.), 3554.

without having to prove anyone's fault is often intended as if society must bear the costs of these social activities[509].

Structurally, strict liability is maybe closer to extra-contractual/tort liability (or negligence, in a more common law framework)[510] because everyone is expected to act with care. However, some risks can develop into harmful facts or actions (or omissions) without the liable person being negligent, or displaying the required level of care, but solely due to the fact that the liable person can exercise a meaningful control over the thing/person for which/whom they will be liable for. Nevertheless, for some meaningful application of strict liability such as product liability, the previous reasoning is not completely applicable: it is true that the producer (now with technological advancements of the IoT this is even more true) has control over the object, but in product liability cases there are also contractual relationships involved (e.g., the contract of sale, due to which I own a certain product which will turn out to be defective). As I will explore in Chapter V by discussing the legal models preceding the PLD, some continental law countries had developed an indirect way to better answer the safety issues with products prior to the PLD. They could do this by relying, for instance, on contractual liability remedies which found their source in contract warranties. In particular, French judges developed an extensive interpretation of warranties connected to the sale of goods contract (in particular *la garantie des vices cachés*) and allowing the seller an *action directe* against the producer[511]. A similar phenomenon also happened in the US with the development of the implied merchant warranty theory, at least at the beginning point of the development of product liability rules and with the creation of a Uniform Commercial Code (UCC)[512].

From a model point of view, Van Dam points out that there are three main types of strict liability. They are i) "liability with an extra debtor"[513], ii) liability for a defective object[514] and iii) liability with a limited defence[515]. Some continental law countries do not have an explicit reference to any of these categories in their civil code (such as in the German BGB)[516]; others instead have references for certain categories of people (such as minors, employees) custody of things, dangerous buildings and animals, such as France[517], and finally others, such as Italy, do

[509] Cees Van Dam, "Strict Liability," In *European Tort Law*, Cees Van Dam (Oxford: Oxford University Press,2013), 299.
[510] Franz Werro and Erdem Büyüksagis, "The bounds between negligence and strict liability," In *Comparative Tort Law: Global Perspectives 2nd*, Mauro Bussani and Anthony J. Sebok (Cheltenham, UK & Northampton, USA: Edward Elgar Publishing, 2021), 186.
[511] Geneviève Viney and Patrice Jourdain, *Les Conditions de la Responsabilité 3e éd* in *Traité de Droit Civil*, Jaques Ghestin (Paris: LGDJ, 2006), 836-847.
[512] Richard A. Epstein, *Cases and Materials on Torts* 9th ed (Austin, Boston, Chicago, New York, the Netherlands: Wolters Kluwer, 2008) 754-755.
[513] Cees Van Dam, " Strict Liability," in Cees Van Dam, *European Tort Law*, Oxford: Oxford University Press, 297-302.
[514] Cees Van Dam, " Strict Liability," in Cees Van Dam, *European Tort Law*, Oxford: Oxford University Press, 297-302.
[515] Cees Van Dam, " Strict Liability," in Cees Van Dam, *European Tort Law*, Oxford: Oxford University Press, 297-302.
[516] Geneviève Viney and Patrice Jourdain, *Les Conditions de la Responsabilité 3e éd* in Jaques Ghestin *Traité de Droit Civil* (Paris: LGDJ, 2006), 675.
[517] Respectively Article 1242 of the French Civil Code (FCC) which takes the place of former Article 1384; and Article 1243 FCC concerning animals (former 1385) and 1244 concerning buildings.

have references similar to the French model rules about things in custody (2051 Italian Civil Code, hereinafter ICC), animals (Article 2052 ICC) dangerous buildings (2053 ICC), but also for minors, employees (Articles 2048, and 2049 ICC) and finally, for dangerous activities (Article 2050 CC). In particular, in Italy, this last article was used also to cover cases of damages caused by new technologies prior to the GDPR being introduced. For instance, liability for violation of the Data Protection Directive (DPD) in Italy was connected to Article 2050 ICC, as a violation of a dangerous activity (data processing). After the introduction of GDPR, Article 82 GDPR on liability was not expressly transposed, hence the majority opinion among legal scholars is that it should be bound by the general rules concerning extra contractual liability set in Article 2043 ICC[518].

As far as harmonization of strict liability at the EU level, this kind of liability is perhaps the most harmonised, as the PLD has been applied in the relationships between consumers and producers of consumers' objects for more than 35 years[519]. It is considered to belong to the strict liability family. The harmonization of national product liability regimes was not a smooth process for some MS, as I will explain in Chapter V. Despite what is written above, in the PLD the criterion for the allocation of liability to the defendant is that the plaintiff (whoever endured the damage) must prove that there is a causal link connecting their damage to the fact or omission from which the pain and suffering derives[520]. In this sense, the PLD is maybe closer to the classical extra-contractual-tort liability scheme than the strict liability-objective one. As I will explain in Chapter V, this was due to the fact that it was conceived not as a consumer protection mechanism, but as an Internal Market facilitator, which needed to also balance out the legitimate interests of producers and manufacturers[521]. Even considering these preliminary considerations on the PLD, EU countries regard the EU product liability directive (PLD) as a form of strict liability, as there is no fault to prove, even if the plaintiff must provide evidence of the causal link, a specific kind of damage and the originating fact[522].

From now on, when I discuss strict liability, I will always refer to liability introduced by the PLD[523].

III. Contractual liability

[518] See more the subparagraph on Future Article 9 PLD, Chapter V.
[519] Piotr Machnikowski, "Conclusions," In *European Product Liability: An Analysis of the State of the Art in the Era of New Technologies*, Piotr Machnikowski (Antwerp-Cambridge-Portland: Intersentia, 2016), 669-705.
[520] Manuela Rinaldi, "RESPONSABILITÀ OGGETTIVA IN GENERALE," In *Trattati Giuridici Omnia-La Responsabilità Civile, vol III*, Paolo Cendon (Torino: Utet Giuridica, 2020, 2nd ed.), 3539
[521] See §§17 and ff. "Commission of the European Communities v French Republic,Case C-52/00," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62000CJ0052.
[522] Article 4 PLD
[523] Piotr Machnikowski, "Conclusions," In *European Product Liability: An Analysis of the State of the Art in the Era of New Technologies*, Piotr Machnikowski (Antwerp-Cambridge-Portland: Intersentia, 2016), 669-705.

Not surprisingly, the contract is one of the most important sources of liability, even at an EU level. As contract law is at the basis of trade, it comes as no surprise that legal scholars (such as Professors Lando and Gandolfi)[524], and also the EU and its predecessors, such as the EC[525], tried to align European contract law, or at least to create an optional instrument based on contract law to achieve completion of the internal market[526]. One of the main achievements was to combine the input that the Commission gave as far as the objective of the harmonization of contract law was concerned with the decade-long work of private law scholars all over the EU. The Draft Common Frame of Reference (DCFR) represents the legal ambitions of that time. Christian von Bar led the DCFR project that resulted in a set of principles ranging through several aspects of private law (including contract law) presented in the form of a code and bringing together the principles of the Lando Commission principles, the existing *acquis communautaire* and also important concepts of property law[527]. Despite the DCFR never becoming a common EU civil code, it was used as a fundamental basis for the drafting of the Common European Sales Law (CESL). It was supposed to be an optional instrument, but MS questioned the extent of the matter handled in the proposed regulation, on the grounds of a lack of convincing rationales, with the exception of the one to improve the functioning of the internal market[528]. Some argued that it was too extended and that, *de facto*, it introduced a sort of EU civil code, disguised as an optional instrument[529]. This project sank after the Barroso's Commission ended. The Commission led by Juncker decided to take a closer look at the developments of the Digital Markets, but the projects that were prior to the CESL, such as the Draft Common Frame of Reference and the Acquis project can nowadays be used as a valuable starting point to harmonise legislation in contractual matters.

[524] Professor Ole Lando created a team of legal scholars who created the Principles of European Contract Law (PECL). The team tried to overcome national differences and to reach an understanding concerning the common core of EU contract law. Conversely, the *Avant-Projet* of a *Code Européen des Contrats* directed by Professor Gandolfi relied mainly on Professor Gandolfi's endeavour and took as a reference mainly Italian civil law and a draft for a Contract Code for the English commission. Nils Jansen and Richard Zimmermann, "General Introduction. European Contract Laws. Foundations, Commentaries, Synthesis," In *Commentaries on European Contract Laws* Nils Jansen and Richard Zimmermann (Oxford: Oxford University Press, 2018),[10]-[23].

[525] In particular, in 2007, the Acquis group published the first principles concerning the EU consumer Acquis (in particular the part on contract was published in 2009). More importantly, the Commission had given input to create a document called Draft Common Frame of Reference (for contract law) and that was achieved. It was substantially the combination of the PECL and the Acquis group results. Nils Jansen and Richard Zimmermann, "General Introduction. European Contract Laws. Foundations, Commentaries, Synthesis," In *Commentaries on European Contract Laws*, Nils Jansen and Richard Zimmermann (Oxford: Oxford University Press, 2018) [10]-[23].

[526] see infra the discussion subsection 2.2 on the application of Article 114 TFEU.

[527] Michele Graziadei, "Fostering a European legal identity through contract and consumer law," in *Research Handbook on EU Consumer and Contract Law*, Christian Twigg-Flesner (Cheltenham, UK, Northampton, USA: Edward Elgar publishing, 2016):91.

[528] Adam Cygan, "A step too far? Constitutional objections to harmonization of EU consumer and Contract Law," In *Research Handbook on EU Consumer and Contract Law*, Christian Twigg-Flesner (Cheltenham, UK, Northampton, USA: Edward Elgar publishing, 2016):24-28.

[529] Nils Jansen and Reinhard Zimmermann, "A EUROPEAN CIVIL CODE IN ALL BUT NAME": DISCUSSING THE NATURE AND PURPOSES OF THE DRAFT COMMON FRAME OF REFERENCE, *Cambridge Law Journal* 69,1 (2010): 98, https://dx.doi.org/10.1017/S000819731000019X.

As of today, there is no explicit general idea of EU contract nor of contractual liability: as a matter of fact, the EU body of contract and consumer law "*is not a comprehensive system but supplement the contract law of MS*"[530]. Also, from a linguistic point of view, the different legal traditions and languages of the EU make it impossible to create perfect equivalences in contract law, as the contents do not necessarily overlap, even if words such as "contratto", "contract" or "contrat" might sound very similar[531]. The same can be said for contractual liability in general in EU consumer and contract law.

Even if EU law does not explicitly mention how to structure contractual liability, this does not mean that some features of an EU contractual liability regime are not starting to emerge. By analysing the directive on late payments, the CESL, the PECLS (Lando Commission principles) and two judgments of the EU[532], Mazzamuto identified that contractual liability from secondary EU law can have the following features: that there must be a) the pre-existence of an obligation/ duty; b) followed by the emergence of three different outcomes which are absolute non-performance, defective performance and delay as a consequence of the breach of the aforementioned obligation-duty; c) the legal effect after one of the events described in b) happened often coincides with monetary compensation and d) the fact that compensation extends also to personal and not only economic/material damage[533]. This perspective might be more Continental law-centred, as it is important to notice that in common law countries, breach of contract plays a central role, whereas "[…] *continental law systems see the contract both as a legal act with its obligations and the liability that this entails derives from the non-performance or breach of contractual obligations*[534].

In any case, considering the corpus of the directives and regulations concerning consumer and contract law, contractual liability is in a somewhat unusual position: there is no doubt that from a quantitative point of view, there are many legislative acts involving contractual and consumer aspects and the introduction of new remedies, such as the right to withdraw, or consumer warranties. What it is still lacking nowadays is a clear-cut EU definition of contract, its elements and how liability is structured. This is also true for some of the newest legislative acts concerning contractual liability, such as the already-cited Directives 2019/770 (DCDS) on the supply of digital content and services and 2019/771 on the sale of goods including the ones with digital elements (SDG).

---

[530] Reiner Schülze and Fryderyk Zoll, *European Contract Law*, 3rd ed (Baden-Baden: Beck-Hart-Nomos, 2021):40.
[531] Hugh Beale, Bénédicte Fauvarque - Cosson, Jacobien Rutgers and Stefan Vogenauer, *Cases Materials and Texts on Contract Law- Ius Commune Casebooks for the Common Law of Europe 3rd* (Oxford: Oxford Hart Publishing, 2019) 93.
[532] Notably Tacconi v. Wagner and Graz Stadt v. Strabag AG according to Salvatore Mazzamuto, *La responsabilità contrattuale nella prospettiva europea* (Torino: Giappichelli, 2015):7.
[533] Salvatore Mazzamuto, *La responsabilità contrattuale nella prospettiva europea* (Torino: Giappichelli, 2015):7.
[534] Reiner Schülze and Fryderyk Zoll, *European Contract Law*, 3rd ed (Baden-Baden: Beck-Hart-Nomos, 2021): 241, hereinafter, Schülze and Zoll.

IV. Pre-contractual liability

At the moment there is no mention of pre-contractual liability *per se* in EU legislation. Nevertheless, the different scholarly projects mentioned, such as the Acquis Principles, the DCFR and the CESL included sets of pre-contractual duties. However, in EU legislation there are rare mentions of "good faith" before concluding a contract and it is rare that there are sanctions or remedies for the breach of these duties[535]. This is due to the MS having opposite views on the importance of this kind of liability and on more or less collaborative visions of society[536]. Common law countries are quite sceptical about whether one should apply good faith when the contract is not yet concluded, while others, notably Italy and Germany, had always had the idea that the parties have mutual duties of good faith and fair trading even before the contract existed[537].

In any case, the most used types of pre-contractual duties are information duties. The reason for their success is also due to their "ecumenical nature": they were easily acceptable, both by neo-liberal ideology and by a more social one, which aimed to increase consumer self-determination[538]. However, findings in behavioural economics and psychology have shown that, especially in digital markets or for complex digital objects, having more information does not always allow the most informed and right choices to be made[539]. This has already proved right with the new forms of nudging and subliminal persuasions (that should be banned through the AIA, if approved, and DSA) that many important actors use through algorithms and facilitated by the use of the IoT.

With regard to the consequences of infringing these pre-contractual duties, there is often the possibility that other remedies (such as withdrawal rights) are extended for a longer period of time. As far as compensation and deciding which kind of pre-contractual liability is more similar, the CJEU established in the *Embassy Limousine* case that the kind of compensation to correspond to violation of pre-contractual liability will follow the rules of tort liability[540]. However, legal scholars have since pointed out that it is indeed difficult to sanction the breach of information duties as it is left to the MS to implement[541].

Overall, in terms of harmonization, pre-contractual duties and obligations are more harmonised as far as their content is concerned, but problems still persist concerning their effective enforcement.

---

[535] Schülze and Zoll, 113-122.
[536] Schülze and Zoll,116.
[537] Schülze and Zoll, 116-117.
[538] These have found place in several consumer directives such as the Door Step Selling Directive, the Consumer Rights Directive. Christoph Busch, "The Future of pre-contractual information duties" In *Research Handbook on EU Consumer and Contract Law*, Christian Twigg-Flesner (Cheltenham, UK, Northampton, USA: Edward Elgar publishing, 2016): 221-223.
[539] Christoph Busch, , "The Future of pre-contractual information duties" In *Research Handbook on EU Consumer and Contract Law*, Christian Twigg-Flesner (Cheltenham, UK, Northampton, USA: Edward Elgar publishing, 2016): 231-240.
[540] Schülze and Zoll, 122.
[541] Leonike Tieglaar, "How to Sanction a Breach of Information Duties of the Consumer Rights Directive?," *European Review of Private Law*, 27 1 (2019): 25-57.

1.2. Liability: risk and innovation

One of the social reasons that underpins the scope of this research also concerns the connection of liability, and product liability in particular, to innovation. The economic analysis of the law is among the best-known methods to concretely measure the impact of liability rules on technology and innovation in general. It is clear from the methodology that this thesis does not wish to analyse the connection of economics with competition and IP law (which primarily relates to technological innovation under different aspects). Nevertheless, I consider that it is important to summarise why the study of product liability from a more economic point of view is able to influence both companies (especially their plans to market a certain technological product, such as an IoT for the home) and consumers/users (e.g., how the price corresponding to a certain IoT product for the home could influence a person's decision to buy or not to buy a certain object)[542].

The very core of the economic analysis of the law, which in the EU is mostly studied in relation to competition law methods to ascertain infringements, is that legal rules can be studied through economic models[543]. The effect is that relying on these economic models could give more accurate predictions on what the consequences of legal acts and policies will be. The American model of economic analysis of the law, translated in terms of risks management, is more focused on the most effective allocation of all risks in society[544], more than on social welfare. Originally, in the USA, despite the specific differences from one scholar to another, the main division from where an economic efficient assessment of a legal system is started is to consider the division between property and liability rules. Calabresi and Melamed considered that liability's function was to protect "people's entitlements" through a third and impartial party, the State, which can calculate the value of the damage or unwanted transfer of said entitlement[545]. Kaplow and Shavell instead concentrated on the fact that liability rules were consequences of harmful externalities, at least most of the time[546]. One of the main subjects of interest of this kind of economic analysis of the law is tort law and its connection to innovation (including strict liability theories and others connected to product liability)[547]. However, another subject of interest

[542] On this issue, see more on 1.4 of this chapter.
[543] Steven Shavell, *Foundations of Economic Analysis of the Law*, (Cambridge, Massachussets-London: The Belknap Press of Harvard University Press, 2004), 4.
[544] Hans-W. Micklitz, "Risk, Tort and Liability," In *New Private Law Theory* Stefan Grundmann, Hans-W. Micklitz and Moritz Renner (Cambridge: Cambridge University Press, 2021), 275.
[545] Guido Calabresi and A. Douglas Melamed, "Property Rules, Liability Rules, and Inalienability: One View of the Cathedral," *Harvard Law Review*, 85,6 (1972), 1092.
[546] Louis Kaplow and Steven Shavell, "Property Rules Versus Liability Rules: an Economic Analysis," *Harvard Law Review* 109,4(1996):716.
[547] Gideon Parchomovsky and Alex Stein, "Torts and Innovation," *Michigan Law Review* 107,2(2008):286-316; William Kip Viscusi and Michael J. Moore, "Product Liability, Research and Development," *Journal of Political Economy* 101,1(1993):161-184.

here is the overall system of rules concerning intellectual property[548] and how disruptive innovation can influence the IP law system.

Because of technological convergence[549], which is leading to a fusion of different technologies through interoperability[550], parts of law that were once more separated will now often be considered together. I argue that this is what will happen with product liability and the intellectual property aspect connected to IoT domestic objects. A balanced legal liability model, including product liability, is of essential importance for companies in terms of the investments they will need to make in R&D, but also in terms of the safety features to add to the product and in terms of insurance against the most frequent and harmful kinds of damages.

1.3. Liability: a balance between different actors

One more reason to study the product liability of IoT objects is because it can also give us a sociological insight into how the different production processes evolved during the last twenty years and how they have led to the success of IoT technology for the smart home.

If we try to analyse the distribution of liability by considering the production/manufacturing process of the IoT for the home, one preliminary matter must be acknowledged: we do not live in a "pure" bricks and mortar economy anymore. Non-connected objects will still exist, of course. Despite that, especially commercial IoT objects for consumers are becoming increasingly more common in households and their "boom" is likely to occur in the next five years[551]. The multitude of objects and their adaptability to any home context was shown implicitly in chapter II with the tentative taxonomies to categorise the domestic IoT. Furthermore, some platforms and Internet services that we can access through domestic IoT objects have turned these same IoT object into gateways that are acquiring the status of increasingly essential commodities. In the future, the expansion of domotics could especially benefit vulnerable people, such as the elderly, but also people with disabilities, as now there is more and more attention on the fact that technology must be accessible to all people, especially

[548] William M. Landes and Richard A. Posner, *The Economic Structure of Intellectual Property Law* (Cambridge-Massachussets, London-England; 2004).
[549] Gerry Kranz, "Technological Convergence," *Tech Target*, Accessed 31 January 2023, https://www.techtarget.com/searchdatacenter/definition/technological-convergence.
[550] Urs Gasser and John Palfrey, "Fostering innovation and trade in the global information society: The different facets and roles of interoperability" In *Trade Governance in the Digital Age-World Economic Forum*, Mira Burri and Thomas Cottier (Cambridge; Cambridge University Press, 2012),124-137.
[551] (3) of the "Commission Staff Working Document Accompanying the Document REPORT FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT Final report- Sector inquiry into consumer Internet of Things, SWD/2022/10 final" EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022SC0010&qid=1653852206944. Martin Armstrong, " The Market for smart home devices is expected to boom over the next 5 years," *World Economic Forum* in collaboration with *Statista* 29 April 2022, Accessed Accessed 31 January 2023, https://www.weforum.org/agenda/2022/04/homes-smart-tech-market/.

in a home environment[552]. Apart from smart phones, the last three years have seen the rise of integrated voice assistants, which have become key-points in the smart-home as far as interaction with the user/consumer and possibly with other objects[553] is concerned. Living without them is still possible but it might make life more complicated than it could be.

Commentators have created several names, such as "the digital revolution"[554] or the "algorithmic society/governance"[555], to describe this new era of "connectedness". The first label emphasises the fact that the divide between a physical world and a digital one is becoming increasingly blurred. The IoT is the technology that makes the border between digital and physical more uncertain and even its unstable definition is maybe the sign that it will remain a "fuzzy" concept[556]. The second label focuses on automated decision-making algorithms that are generally not an integrated part of the IoT objects, but still have an influence on them, at least from the cloud. Nevertheless, there are already exceptions for home IoT: voice assistants are algorithm-led programs which are particularly trained in Natural Language Processing (NLP) and their physical appearance is requested but not necessarily connected to just one type of physical object[557].

In the last forty years, the structure of the Internet has changed the economic productive structure by partly transferring its characteristics, such as its decentralised original structure, and by creating new ones. This has been achieved, for instance, by connecting markets that had previously been more connected to electricity than to automatisation and the Internet, such as smart appliances and smart objects for the home. Since its origin, the Internet has required several actors which were tied by different kinds of relationships of agency (users, servers-owners and different intermediaries, the most famous of which were the Internet Service Providers, now known by the terms of VLOPS[558] and VLOSES[559] in the DSA, and core platform services or gatekeepers, according to the DMA[560]). The core function of the Internet, which is a telecommunication technology, is still to break down information into small

[552] This belief/trend has also prompted the development of new models that are mindful of the age and the disabilities of potential users. See Joong Hee Lee et al., "A persona-based approach for identifying accessibility issues in elderly and disabled users' interaction with home appliances," *Applied Sciences* 11,1 (2021):368, https://dx.doi.org/10.3390/app11010368.
[553] (43)-(47) Commission Staff Working Document- Report on the Consumer IoT.
[554] Luciano Floridi, *The 4th Revolution* (Oxford: Oxford University Press, 2014).
[555] Marc Schuilenburg and Rik Peeters, "The Algorithmic Society. An Introduction," In The Algorithmic Society. Technology, Power and Knowledge, Marc Schuilenburg and Rik Peeters (Routledge:London, 2020), 2 ,https://dx.doi.org/10.4324/9780429261404 .
[556] As already cleared in Chapter I.
[557] Félix Le Pailleur, Bo Huang, Pierre-Majorique Léger and Sylvain Sénécal, " A New Approach To Measure User Experience with Voice-Controlled Intelligent Assistants: A Pilot Study," In *Human-Computer Interaction. Multimodal and Natural Interaction. HCII 2020. Lecture Notes in Computer Science*(), vol 12182. Kurosu, M. (Cham, Switzerland :Springer Cham, 2020):197-208; Sakshi Gupta, " Natural Language Processing Use Case- How Do Personal Assistant Apps Work?," *Springboard*, June 10, 2020, Accessed 31 January 2023, https://www.springboard.com/blog/data-science/nlp-use-cases/.
[558] Very Large Platforms.
[559] Very Large Online Search Engines.
[560] For a more accurate description of VLOPS, VLOSES and Gatekeepers see the parts on the DMA and DSA in Chapter III.

packages and to send each of them through different paths and then reassemble them in the correct order for the recipient of the message[561]. Furthermore, people are used to thinking about the Internet as a collective entity but in reality there are many Internet structures[562]: there is one tangible Internet which is made up of the telecommunication structure that carries messages; then there is the ensemble of bytes that composes the structured information and that is transmitted through different internet protocols[563]. Some commentators have already pointed out that one of the characteristics of our times is the proliferation of intermediate bodies, such as platforms [564]. These intermediate bodies are mostly used in order to access services or obtain goods further to payment of money, or paying by providing our information and data, personal or non-personal[565]. Because of the network effects of a digital economy[566], new situations of imbalances of power have emerged[567], and principles that at the start were thought to be immutable do not now apply anymore. Now, whoever does something for the first time is able to quickly develop network externalities (meaning that the convenience of a technology grows with the increasing number of users) and it is quite rare that a competitor with a better product/service can succeed more than the first developer of the idea[568].

One difficult concept in understanding how the value-chain and supply-chain for the IoT are structured is that basically there will be a different model for each new object. However, it is possible to make some generalisations with two macro models.

1 model: a platform or Internet search engine designs the new product (such as the voice assistant). It is then produced by a) company branches b) contractors c) a mix of a) and b). Let us bear in mind voice assistant objects as an example for this.

2 model: a producer or manufacturer which could be a) already on the market b) incumbent, with the objective of creating and marketing an IoT domestic object that can be a) a completely new product (e.g., a cleaning robot) b) an upgraded domestic object (a smart fridge). The second model is the most problematic because of three factors: a) it can have several different contractors

[561] Chris Reed, *Internet Law. Text and Materials, second edition.* (Cambridge: Cambridge University Press, 2004), 7-23.
[562] Chris Reed, *Internet Law. Text and Materials, second edition.* (Cambridge:Cambridge University Press, 2004), 7-23.
[563] Chris Reed, *Internet Law. Text and Materials, second edition.* (Cambridge:Cambridge University Press, 2004), 7-23.
[564] Marco Ricolfi, "Il futuro della proprietà intellettuale nella società algoritmica", *Giurisprudenza Italiana*, (2019): 18-21.
[565] For instance, the SDG, the DCDS, the Free Flow of Data and the Data Act.
[566] Jacques Crémer, Yves-Alexandre De Montjoye and Heike Schweitzer, *Competition policy for the digital era* (Luxembourg: European Commission, 2019),1-10, Accessed 31 January 2023, https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf .
[567] Jacques Crémer, Yves-Alexandre De Montjoye and Heike Schweitzer, *Competition policy for the digital era* (Luxembourg: European Commission, 2019),1-10, aAccessed 31 January 2023, https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf .
[568] Jacques Crémer, Yves-Alexandre De Montjoye and Heike Schweitzer, *Competition policy for the digital era* (Luxembourg: European Commission,2019),1-10, aAccessed 31 January 2023, https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf .

making physical or software parts for the objects b) it may rely on a huge platform or search engine, also for interoperability's sake c) it may also need a cloud service for storage or data processing, which may (or may not) coincide with the proprietary clouds of the platform or search engine with which the object should be interoperable.

At the moment, the only legal model that allows us to deal with this more complex value and supply chain is the paradigm offered by the GDPR of controller and processor. As already explained in Chapter III, the controller is always liable in principle for lack of accountability according to Article 5(2) GDPR, but also for damage caused by any kind of violation of the GDPR, as the division between the two roles is dictated in terms of delegated activities by the controller to the processor. Theoretically, this division could also help to list the situations of joint controllership[569], which would inevitably arise in a connected environment and might make it quite complex. For instance, let us consider that a producer of automated blinds might have made arrangements with a voice assistant manufacturer (Samsung, Google, Apple, or Amazon) to make its system interoperable. The personal data or information collected by the voice assistant could be partly shared with the smart appliance producer and vice versa. Based on specific contracts, this model only applies to personal data and has been criticised for being practically impossible to implement[570] especially in a future fully connected environment, where one product could interact with another and process personal data, with both the smart product manufacturers being unaware of this. Alternatively, the data subject and its home guests might become part of the data controller's group due to of the restrictive application of the household exemption in Article 2(2)(c) GDPR[571].

The staff working document accompanying the final report of the Commission's sector inquiry into the consumer internet of things had also pointed out another important problem: that voice assistant producers (in our scheme, they would be one of the model 2 sub-scenarios) were able to impose interoperability and contractual conditions on the consumer IoT object manufacturers[572]. This could potentially lead to market distortions and, consequently, less choice for consumers from a competition point of view. It would therefore appear that this situation was at the origin of the rationale of Article 13 of the Data Act, which basically sanctions the imposition of unfair terms with invalidity, following the model of the previous Unfair Contract Terms Directive. Also, there are two lists of contract clauses that are presumed to be unfair. This article seems not only to apply to the new data sharing paradigms in Article 4 and 5 of the Data Act (DA), but also to any contract term that has been "unilaterally imposed" and that concerns data use, access and related remedies. Hopefully Article 13 DA will help to solve this problem, but it is still unclear how it would be enforced, especially if we consider that the value and supply chains of

[569] Article 26 GDPR.
[570] Michèle Finck, "Cobwebs of control: the two imaginations of the data controller in EU law," *International Data Privacy Law* 11,4(2021):333-347, https://dx.doi.org/10.1093/idpl/ipab017.
[571] More in Chapter III, sub-sub-section 2.1.
[572] Staff Working Document Accompanying REPORT –Consumer IoT (2022), 10-11.

home IoT objects is not limited to the EU but mostly extends to Asia and America. We will only witness in future whether both Article 3 GDPR and Article 2(1)(a) of the proposed DA, which ensure application of data protection and the rules on sharing data whenever the data processing/sharing service is offered in the EU, will be able to lead to an effective enforcement.

In conclusion, at least in the EU, the complexities of the supply and value chains concerning the production of home IoT objects are starting to be taken into account. First of all, implicitly with the GDPR, then more explicitly with the proposed Data Act. Both these models are regulatory, and lean more towards administrative than private law, at least in theory. It is likely that if material or immaterial damage occurs due to a GDPR violation of a home IoT product, it will be more likely to consider the controller liable, even if data are non-personal, as it is, in general, the stakeholder that delegates its function to others. This allocation of liability seems fair when considering a situation such as the one described in model 1, as, generally, the delegating entity is a multinational company with sufficient economic resources. With regard to model 2, the delegation of tasks concerning both personal and non-personal data does not imply that the controller/delegating subject has *de facto* more power or resources. In order to correct the imbalances of power, Article 13 of the proposed Data Act adapts remedies and techniques from the European consumer and contractual *acquis* to data contracts. Nevertheless, this article can be applied in solely a contractual liability context, which is more than satisfactory when one considers the relationship between the various stakeholders involved in home IoT object production. However, given that users are an essential part of the functioning of these objects, the lack of a form of subdivision of liability among the many actors in the IoT product chain risks damaging the confidence and trust that users and consumers have in these objects. The actual PLD remains silent on the IoT production chain for consumer objects. That is why, for businesses, it would be beneficial to have a clearer view on the allocation of this particular kind of strict liability.

1.4. Liability: an enhancer of trust in IoT technology for the home

It is difficult not to associate legal liability, and especially product liability, with litigation. However, if we also intend liability as the possibility to have access to effective remedies, one of the consequences for users will be to increase trust in technology. I argue that trust, especially in the smart home, is not only increased by the progressive unfolding of our beliefs in the capabilities of a smart object[573], which can be substantially improved by the object offering good usability[574] and accessibility for all different users. It is also increased by a system of effective remedies such as liability. This has also been mentioned by the High

[573] Mariarosaria Taddeo, "Modelling trust in artificial agents, a first step toward the analysis of e-trust," *Minds & Machines* 20,2(2010): 243-257, https://dx.doi.org/10.1007/s11023-010-9201-3 .
[574] See Chapter 2.

Level Expert Group on AI in its ethical guidelines for the development of AI[575]. It is a pity that the document concentrated only on ethical and cybersecurity aspects and not legal ones as it would have been useful to comment on liability principles. In any case, having a product liability directive that sets the parameters for which kinds of damages could be compensated and which conditions would incentivise consumers to buy these objects as they would finally trust them.

1.5. Liability in a home that changes: how perceptions of the home environment have changed and their impact on liability

In Chapter II, I provided a concise description of how smart home technology primarily had either an energy-saving or an automatisation function at its origin. Problems in its adoption by elders and the insufficiency of computational power created long-term discouragement from investing in a home that was truly connected as an entirety and not as a piece-meal ensemble of IoT objects, as a growing number of households has these days[576]. Nevertheless, the COVID-19 pandemic has been and still is a major factor concerning the creation of a more connected and adaptable smart-home[577]. Could it contribute to a new definition of smart home? Would it be different from a simple connected environment? What I will argue in this subsection is that, to display its potential, the future smart home has to become a real tool for environmental sustainability and social inclusion, thus also influencing the concept of product liability we have today. There are hints that indirectly point to this trend. For instance, there is an increasing amount of "green" "eco-sustainable" corporate objectives[578] and voluntary, "green" international certifications, such as the EU legislation on eco-labels[579]. The origin of these phenomena is 2030 Sustainable Development Goals (SDG)[580] and the ever more serious climate crisis.

As a starting point, during the first year of the COVID-19 pandemic, the home quickly became (and still is in part at the moment of writing) the major centre of the life of individuals, whether they were data subjects, consumers or professionals. Sociological studies also showed that, for some, the home has

[575] AI HLEG, "Ethics Guidelines for Trustworthy AI," (2019), Accessed 31 January 2023, https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.
[576] See Chapter 2.
[577] Chris Marlin, "How Covid-19 will change the way we design our homes," *World Economic Forum*, August 3, 2020, Accessed 31 January 2023, https://www.weforum.org/agenda/2020/08/how-covid-19-will-change-what-we-call-home-ddfe95b686/.
[578] Andrew Winston, "Sustainable Business Went Mainstream in 2021," *Harvard Business Law Review*, 27 December 27, 2021, Accessed 31 January 2023, https://hbr.org/2021/12/sustainable-business-went-mainstream-in-2021. The fact that most companies decided to adopt a "green" and "sustainable attitude" also spread many doubts about the authenticity and sincerity of this message, making it quite difficult to tell apart a sustainable corporate endeavour from greenwashing, meaning when a company makes unsubstantiated sustainability claims. Bruce Watson, "The troubling evolution of corporate greenwashing," *The Guardian*, August 20, 2016, Accessed 31 January 2023, https://www.theguardian.com/sustainable-business/2016/aug/20/greenwashing-environmentalism-lies-companies.
[579] European Commission, "EU-Ecolabel," Accessed 31 January 2023, https://environment.ec.europa.eu/topics/circular-economy/eu-ecolabel-home_en.
[580] UNDP, *Sustainable Development Goals*, Accessed 31 January 2023, https://sdgs.un.org/goals.

become a small city within a few walls[581]. In particular, tele-work[582] has become mainstream and is an actively used tool even today. However, a relevant number of homes in urban and suburban areas were not ready for the "widening" of the home's functions when the pandemic began. Some households did not have access to high-speed internet (through optic fibre) or were not equipped with a sufficient number of monitors and devices that enabled the inhabitants to work or study. Thus, previous social inequalities have unfortunately persisted also in terms of disparity of access to essential technology[583]. The incremental blurring of a "traditional" work-life division in the home had a disruptive effect as the majority of current homes, especially in urban environments, were designed with the consideration that most social life was taking place outside the home[584]. Oftentimes, during the beginning of the pandemic, more than two individuals had to share a restricted space for an increased number of functions including entertainment, physical exercise, socialisation and spirituality[585].

[581] In particular, urban scientists, sociologists and architects called upon governments to consider that space is essential in the impact of the inhabitants' wellbeing in connection with the blurring of the work-home division. Jenny Preece et al., "Urban rhythms in a small home: COVID-19 as a mechanism of exception," *Urban Studies* (2021): 2, https://dx.doi.org/10.1177/00420980211018136. On the importance of space in the home "…as contemporary domestic architecture is no longer centred on the emotional and material needs of human beings".

[582] Teleworking was so crucial during the pandemic that two major international organisations such as WHO and ILO created a joint report about the impact of telework on workers' health. In particular, if better quality time with family and pets without commuting could be achieved by teleworking, the absence of a specifically conceived work station could cause an insurgence of pain (5) ILO and WHO, *Healthy and Safe Telework. Technical Brief- Geneva,* 2021, 5, Accessed 31 January 2023, https://www.who.int/publications/i/item/9789240040977.

[583] Unfortunately, it appears that, since the start of the pandemic, pre-existing social disadvantages have stayed the same, when gaps have not shrunk in housing and access to new and essential technologies. Yung Chun and Michal Grinstein-Weiss, "Housing inequality gets worse as the COVID-19 pandemic is prolonged," *Brookings Edu*, December 18, 2020, Accessed 31 January 2023, https://www.brookings.edu/blog/up-front/2020/12/18/housing-inequality-gets-worse-as-the-covid-19-pandemic-is-prolonged/; Vincent Bernard et al., " Logements suroccupés, personnes agées isolées…: des conditions de confinement diverses selon les territoires," *INSEE FOCUS* 189, 21 Avril 2020, Accessed 31 January 2023, https://www.insee.fr/fr/statistiques/4478728 . Differences also emerged in terms of relationship with "screen-time" within the same households, see Jocelyn Lachance, "Sommes-nous égaux face aux écrans en période de confinement?," *The Conversation*, April 19, 2020, Accessed 31 January 2023, https://theconversation.com/sommes-nous-egaux-face-aux-ecrans-en-periode-de-confinement-136130. To understand how poverty determined access to school and learning technologies in Italy see Osservatorio Povertà Educativa-Openpolis- Con i Bambini, *Disuguaglianze digitali. Bambini e famiglie tra possibilità di accesso alla rete e dotazioni tecnologiche nelle scuole* 35, 2020, Accessed 13 February 2022, https://www.openpolis.it/wp-content/uploads/2020/07/Disuguaglianze-digitali.pdf.

[584] Marco Aresta and Nikos A. Salingros, "The Importance of Domestic Space in Times of COVID-19," *Challenges* 12,2 (2021):28, https://dx.doi.org/10.3390/challe12020027.

[585] Marco Aresta and Nikos A. Salingros, "The Importance of Domestic Space in Times of COVID-19," *Challenges* 12,2 (2021):28, https://dx.doi.org/10.3390/challe12020027.

As a consequence, the real estate market[586], interior design and architecture[587] started to change. To begin with, people were trying to find homes that were maybe in suburban areas, closer to spaces such as gardens or parks where they could feel less constricted, and it seems that this tendency has not yet stopped[588]. If that was not possible, people were trying to create "greenery" spaces[589] within their living environment, such as small *vegetable plots*, in order to have fresh supplies of herbs and small vegetables or fruits. Another green-increasing technique was the decoration of balconies with plants. Balconies are now seen as a plus point for people living in urban areas. Interior design also started to inquire how to re-arrange and re-adapt existing spaces according to the functions of the day[590]. Architecture and domotics united forces in order to draft guidelines on how to build a truly connected smart home[591], also keeping in mind the necessity to reconvert the home environment for a diverse number of functions, including entertainment. Interestingly enough, AI-IoT hybrid technologies which allow users to experience virtual reality or the metaverse are also now one of the most frequent causes of technology related-domestic accidents[592]. Moreover, it is assumed that during the pandemic the relationship

[586] The real estate market for homes in the EU, as far as investments are concerned, was always increasing as the crisis did not have an economic origin as in 2008-2010, and in the future it should maintain this trend. The ECB noticed that the demand of homes in rural areas increased as well as the decision of families to move from the place where they actually live, chart 8. Niccolò Battistini, Matteo Falagiarda, Johannes Gareis, Angelina Hackman and Moreno Roma for ECB " The Euro area housing market during the COVID-19 pandemic," *ECB Economic Bullettin*, 7 (2021): chart 8 https://www.ecb.europa.eu/pub/economic-bulletin/articles/2021/html/ecb.ebart202107_03~36493e7b67.en.html .

[587] Gestalten, "Henning Larsen: Will the Pandemic Change Architecture?" February 2021, Accessed 31 January 2023, https://gestalten.com/blogs/journal/henning-larsen-will-the-pandemic-change-architecture. Andy Olin, " How will COVID-19 alter today's house of tomorrow,", *Rice Kinder Institute for Urban Research*, January 4, 2021, Accessed 31 January 2023, https://kinder.rice.edu/urbanedge/2021/01/04/Covid-19-trends-home-design-pandemic-work-from-home; Alyssa Giacobbe, "How the COVID-19 Pandemic Will Change the Built Environment," *AD*, March 18, 2020, Accessed 31 January 2023, https://www.architecturaldigest.com/story/covid-19-design.

[588] Anna Stankowska and Izabela Stankowska-Mazur, "The Third Wave of COVID-19 versus the Residential Preferences in Poland: An Assessment of Economic Factors and Psychological Determinants," *Sustainability*, 14,3(2022):1351 https://doi.org/10.3390/su14031339. A tendency that was confirmed by the EBC report previously cited. See also Marta Bottero et al., "New Housing Preferences in the COVID-19 Era: A Best-to-Worst Scaling Experiment," in Osvaldo Gervasi et al, *Computational Science and its Applications- ICCSA 2021* (2021):120-129.

[589] pwc, *Emerging Trends in Real Estate ®: Europe 2022*, Accessed 31 January 2023, https://www.pwc.com/gx/en/industries/financial-services/asset-management/emerging-trends-real-estate/europe-2022.html.

[590] As an example, the Australian architecture firm Woods- Bagot created the AD-APT modulable environments which can transform a home into a work, entertainment and family centre. Simon Saint, "AD-APT: How will buildings adapt to the new realities of home?, " *Woods- Bagot Journal*, Accessed 31 January 2023, https://www.woodsbagot.com/journal/ad-apt-how-will-buildings-adapt-to-the-new-realities-of-home-as/ .

[591]Archdaily, "How to design smart homes. 8 Tips for incorporating domotics into architecture," *Archdaily,* Accessed 31 January 2023, https://www.archdaily.com/908468/how-to-design-smart-homes-8-tips-for-incorporating-domotics-into-architecture and "Smart Home. La Casa Intelligente",*Il Giornale dell'architettura*,Acessed 31 January 2023 https://ilgiornaledellarchitettura.com/2021/09/01/smart-home-la-casa-intelligente/,. Com-Art, 'Maison connectée: les innovations majeures de 2020 en termes de domotique," Accessed 31 January 2023, https://www.comart-design.com/maison-connectee-les-innovations-majeures-de-2020-en-termes-de-domotique/.

[592] Lorenzo Nicolao," Realtà virtuale, crescono gli incidenti domestici: TV rotte, infortuni e "braccio del gorilla"," *Corriere della Sera-LOGIN: TecnologiaInnovazione,* February 15, 2022, aAccessed 31 January 2023, https://www.corriere.it/tecnologia/22_febbraio_15/realta-virtuale-crescono-incidenti-domestici-tv-rotte-infortuni-braccio-gorilla-2ed9360a-8e45-11ec-a91e-e98defcaa657.shtml. A-Hed "VR to the ER:

that users had with technology changed: more people were encouraged to become more digitally literate[593]. Furthermore, within the home, children and old people started interacting more with technology, also due to the development of empathic robotics[594] in some facilities.

At this point, it is interesting to ask how the pandemic-induced transformation of the home is different from, for instance, the late 1990s and early 2000s when PC, laptops, and floppy disks started co-existing with other electronic appliances such as TV, radios, washing machines and vacuum cleaners. When computer technology started to become more mainstream through personal computers (PC), interior design components for the home also changed: there were small furniture structures to host PCs and printers[595]. The adaptation of interior design and home architecture to developing technology is a far from new phenomenon[596]. This had happened before with the introduction of the radio, and, then, with television. Two things seem to have changed with the fast development of the IoT in our homes. The first element is that the pandemic started at a time when ubiquitous technology had already been theorised and its first applications, such as voice assistants and connected appliances, were already available on the market. The second element is that the pandemic was a wake-up call regarding the effects and consequences of climate change on our lives[597]. I believe that these two elements, meaning the pervasiveness of IoT technology for the home and the unwanted consequences of climate change caused by our current economic and productive system, are going to influence product liability for domestic connected objects.

As far as the first element of novelty, meaning the pervasiveness of IoT technology in the smart home, is concerned, there will be consequences both on *i)* the legal subjects and their clear definition in the connected home and *ii)* data

---

metaverse Early Adopters Prove Accident-Prone," *The Wall Street Journal*, February 2, 2022, Accessed 31 January 2023, https://www.wsj.com/articles/metaverse-virtual-reality-vr-accident-prone-meta-11643730489.

[593] Such as teachers and students and also old people. Ming Li and Zhonggen Yu, "Teachers' Satisfaction, Role, and Digital Literacy during the COVID-19 Pandemic," *Sustainability* 14,3(2022):1121, https://dx.doi.org/10.3390/su14031121; Banu Inan Karagul, Meral Seker and Cansu Aykut, "Investigating students' digital literacy levels during online education due to the Covid-19 pandemic," *Sustainability* 13,21(2021):11878, https://dx.doi.org/10.3390/su132111878.
; Igor Kanižaj and Maria José Brites, "Digital Literacy of Older People and the Role of Intergenerational Approach in Supporting Their Competencies in Times of Covid-19 Pandemic," In *Human Aspects of IT for the Aged Population. Design, Interaction and Technology Acceptance. HCII 2022. Lecture Notes in Computer Science,* Gao, Q., Zhou, J. (eds) vol 13330, (Springer, Cham.), 335-345, https://dx.doi.org/10.1007/978-3-031-05581-2_25.

[594] In particular, a promising new field of research is the one of empathic robotics. Marialejandra García-Corretjer, Raquel Ros, Roger Mallol and David Miralles,"Empathy as an engaging strategy in social robotics: a pilot study," *User Modeling and User-Adapted Interaction* 2022 https://dx.doi.org/10.1007/s11257-022-09322-1.

[595] Such as the Lenovo table. Lenovo, " Lenovo tailors horizon table-pc for the home with three fashionable furniture designs," *Lenovo story hub*, May 15, 2013, Accessed 31 January 2023, https://news.lenovo.com/pressroom/press-releases/lenovo-tailors-horizon-table-pc-for-the-home-with-three-fashionable-furniture-designs/.

[596] Kate Wagner, "Machines for Living In: How Technology Shaped a Century of Interior Design," *99% Invisible*, January 13, 2017, Accessed 31 January 2023, https://99percentinvisible.org/article/machines-living-technology-shaped-century-interior-design/.

[597] Colin J. Carlson et al., "Climate change increases cross-species viral transmission risk," *Nature* 607(2022): 555-561, https://dx.doi.org/10.1038/s41586-022-04788-w.

processing influencing not only the rights to privacy and data protection but also the concept of ownership, especially when applied to data. The first consequence, meaning the blurring of the distinctions between the data-subject, the consumer and the professional is increased by the possibility of cumulating all these three functions in the same home and, possibly, some of the three at the same time. If we think about smart domestic appliances as consumer objects that can process our personal data as their main (or most important) function, it is easy to assume that the notion of consumer will almost always overlap with the notion of data subject. The professional definition can also in part overlap with the notion of (most of the times unaware) joint data controller. In Chapter III I highlighted how the restrictive interpretation of the household exemption by the CJEU is leading consumers to be considered data controllers of the personal data shared in their home even by third parties. This may also be the case when the subject is a professional. For instance, lawyers reported that confidential information concerning their clients was listened to by their own voice assistants, with serious problems concerning the principle of attorney-client privilege[598]. In this case, according to Article 26 GDPR, the lawyer and the voice assistant's manufacturer would be joint controllers of their clients' data, and this is something the client-data subject or the lawyer- joint controller might not have explicitly agreed too. The difficulty in distinguishing them is also partly demonstrated by the "rise" of a new legal subject in the latest EU DGA regulation and DMA, DSA and Data Act (DA) proposals: the user, that can be a physical but also a natural person, performing activities on data. One thing that does not help interpreters is that there does not seem to be a uniform definition of user. From the first definition of user in the approved DGA and in the other documents cited (DMA, DSA and DA), there have been small variations concerning its extent that do not help in giving a harmonised interpretation to these different legislative acts. For instance, the GDPR does not have a definition of user, whereas in Article 2(9) DGA, the definition of user is actually "[…] *a natural or legal person who has lawful access to certain personal or non-personal data and has the right, including under Regulation (EU) 2016/679 in the case of personal data, to use that data for commercial or non- commercial purposes*". In the Data Act (DA), instead, Article 2(3) only mentions the user, who is seen mainly in a "data-economy perspective" as it can be "[…] *a natural or legal person that owns, rents or leases a product or receives a service*". In the DA however, this definition coexists with the ones of data holder and of data recipient in Articles 2(6) and (5) DA. Their only point in common with the definition of user is that they could concern both natural and legal persons with the obligation to respectively share personal or non-personal data when asked and/or to receive them according to the DA provisions. The DSA, instead, does not explicitly define the user or data user but makes reference only to the consumer in Article 2(c) by following the EU *consumer acquis*. The DMA, on the other hand, mentions just the end-user as an individual or company who/which uses the platform in a non-business-oriented way in Article 2(16) DMA. Therefore, in a future PLD adapted to IoTs, it is likely that the definition of

[598] Crystal Tse and Jonathan Browning, "Locked-Down Lawyers Warned Alexa Is Hearing Confidential Calls," *Bloomberg Law*, March 20, 2020, Accessed 31 January 2023, https://news.bloomberglaw.com/business-and-practice/locked-down-lawyers-warned-alexa-is-hearing-confidential-calls.

user or data user might be employed. Moreover, as the environment becomes more connected, appliances tend to "merge" with architecture and common objects acquire sensors, people as users and data subjects implicitly give up their privacy in favour of private actors and hence agree to having "reduced" privacy in exchange for goods and services[599]. At the same time, they might also develop new concepts of data ownership: data might be seen as a by-product of a physical object that a person has bought and that they own, especially when "the by-product" takes the form of content that was totally or partly created by the home inhabitant. This is also hinted at by the definitions of both product and related service in the new DA. Product in fact is considered as "[…] *a tangible, movable item, including where incorporated in an immovable item that obtains, generates or collects data concerning its use or environment and that is able to communicate data via a publicly available electronic communications service and whose primary function is not the storing and the processing of data*"[600] . Instead, related service is considered as "[…] *digital service, including software, which is incorporated in or inter-connected with a product in such a way that its absence would prevent the product from performing one of its functions*"[601]. This completes the definition of "goods with digital elements" in Article 2(5)(b) of the Sale of Goods (SDG) directive which were described simply as items which had incorporated or interconnected with digital content or a digital service whose absence would have prevented the items themselves from performing.

Concerning the second element of novelty, climate change and the pandemic will also influence *i)* care and sustainability in the production of IoT objects and also *ii)* the function of the objects being commercialised. As already explained in chapter II, smart homes do not have a specific and tailored sustainability policy at the EU level. There are objectives to make buildings more energy efficient, and the rest is delegated to present consumer and contract law (in particular directives 770 and 771/2019/EU) and the initiatives stemming from the New Consumers Agenda. Climate change will force domestic IoT producers to try to maximise energy efficiency, but also to slow down the rate at which products become obsolete, as instead they do now due to the semiconductors crisis[602]. As noted by Terryn, the actual set of remedies in EU consumer law is not really in line with the objectives of the circular economy and she points out that refurbished goods are outside the field of application of the EU consumer and *contractual acquis*[603]. Moreover, some issues, such as the one regarding independent repair (meaning repair that is not carried out by specialised IoT producers) are not even considered[604]. These are issues that will need to be

[599] Luiz Costa, "Data Protection Law, Processes and Freedoms," In *Virtuality and Capabilities in a World of Ambient Intelligence*, Luiz Costa (Switzerland: Springer International, 2016):137-170.
[600] Article 2(2) DA.
[601] Article 2(3) DA.
[602] See Chapter II and in particular the EU strategy to approve a European Chips Act. "European Chips Act: Communication Regulation Joint Undertaking and Recommendation," *European Commission*, February 8, 2022, Accessed 31 January 2023, https://digital-strategy.ec.europa.eu/en/library/european-chips-act-communication-regulation-joint-undertaking-and-recommendation.
[603] Evelyne Terryn, "A Right to Repair? Towards Sustainable Remedies in Consumer Law," *European Review of Private Law* 4(2019):851-873
[604] Evelyne Terryn, "A Right to Repair? Towards Sustainable Remedies in Consumer Law," *European Review of Private Law* 4(2019):851-873.

considered especially when thinking about any future new product liability directive which will be applied to low-risk technological applications such as IoT objects for the home. Concerning the function of the future generation of connected domestic objects, it is likely that domestic appliances will be increasingly targeted and specialised also according to age groups. Given the statistics of older age groups in Europe[605], this might also impact companies which might decide to have *ad hoc* products with better accessibility, and which integrate exer-games, rehabilitation exercises and other functions for the elderly but who are still autonomous people[606]. It is no secret that global commercial platforms, such as Amazon are already thinking about expanding into the health sector [607]. In legal terms this will mean that there will be a growing number of domestic IoT devices whose function and data processing activities will not just be commercial but also health-related, with more complex duties in terms of compliance with possible interconnections between the PLD, the MDR and the GSOD.

2. Liability in EU private law and the smart home

The directive on certain aspects of the Sale of Goods (including the ones with interconnected digital contents or digital services, SDG) and the directive on the Supply of Digital Content and Digital Services (DCDS), the proposed DSA, DMA and the AI Act have one thing in common: their legal basis, which is the harmonization and approximation of law clause, Article 114 TFEU. However, in the explanatory memoranda of all the documents connected to the European Digital Strategy, the necessary paragraphs concerning the legal basis and respect of the principle of proportionality are rather vague. If the choice of the legal act basis for a proposed PLD is made hastily, it is only a matter of time before it is challenged before the CJEU or some national court. Moreover, history shows, that, although quite rarely, legal acts can be invalidated completely (2.2). The sections below will attempt to explain the structure of Article 114 TFEU and will try to outline why Article 114 may not be the most suitable legal basis for the new PLD.

2.1. The EU criteria for competence: the principle of conferral and the principle of subsidiarity

[605] Eurostat, *Population structure and ageing*. Available at https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Population_structure_and_ageing#Median_age_is_highest_in_Italy, Accessed 31 January 2023.
[606] So Ye Yint Tun, Samaneh Madanian and Frhaan Mirza, " Internet of things (IoT) applications for elderly care: a reflective review," *Aging Clinical and Experimental Research* 33(2021):855-867; Ann Blandiford, Janet Wesson, René Amalberti, Raed Alhazme and Ragad Allwihan, "Opportunities and challenges for telehealth within, and beyond, a pandemic," *The Lancet Global Health* 8,11(2020), https://dx.doi.org/10.1016/S2214-109X(20)30362-4.
[607] Rachel Lerman and Hamza Shaban, "Amazon will see you now: Tech giant buys health-care chain for $3.9 billion," *The Washington Post*, 21 July 2022, https://www.washingtonpost.com/business/2022/07/21/amazon-health-care/ .

Conferral is a founding principle of the Treaties[608]. It means that the EU is competent as long as the MS confer competences on it[609]. The MS decided to determine the distribution of competences in the Lisbon Treaty as they were concerned about a surreptitious growth of competences, as the teleological interpretation of the CJEU had done for fundamental rights in the seminal *Handelsgesellschaft* case[610]. In order to counteract the extensive interpretation and application of shared competences of the EU, the Treaty of Lisbon also provides for respect of the principle of subsidiarity, which made it necessary to involve national parliaments in the legislative procedure[611]. For scholars however, there are at least four dimensions to consider whenever discussing the EU which are "*i) the MS' choice as to the scope of EU competence as expressed in the Treaty Provisions, ii) the MS' and the EP's acceptance of legislation from the Treaty Articles iii) the jurisprudence of the EU courts iv) the decisions taken by the EU institutions as to how to interpret, deploy and prioritise the power accorded to the EU*"[612]. Formally, this explicit distribution of competences and the power given to national parliaments should provide a system of checks and balances, and yet post-Lisbon legislative acts and judgments showed that the repartition of consequences was not as inflexible as intended[613].

At a first glance, it would seem that the Lisbon Treaty created a clearer distribution of competences than before. One of the reasons, apart from the "competences creep", for drafting a clearer distribution of competences was also an alleged mistrust that would derive from an implicit enlargement of EU competences and powers and from a process of excessive centralisation[614]. With

[608] Paul Craig and Gráinne and De Burca, *EU Law. Texts, Cases and Materials (5th edition)* (Oxford: Oxford University Press, 2015),75.
[609] Grainne and De Burca 75
[610] "Internationale Handelsgesellschaft mbH v Einfuhr- und Vorratsstelle für Getreide und Futtermittel, Case C-11/70", EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A61970CJ0011. See also commentary by Bill Davies, "*Internationale Handelsgesellschaft* and the Miscalculation at the Inception of the ECH's Human Rights Jurisprudence," In *EU Law Stories. Contextual and Critical Histories of European Jurisprudence*, Fernanda Nicola and Bill Davis (Cambridge: Cambridge University Press, 2017), 157-177, https://dx.doi.org/10.1017/9781316340479.009.
[611] Article 6(1) TEU and also a dedicated protocol on subsidiarity
[612] Paul Craig and Grainne and De Burca, *EU Law. Texts, Cases and Materials (5th edition)*, Oxford: Oxford University Press, 2015, 74.
[613] In particular, in 2011, during the Greek financial crisis, the setting up of the Emergency Mechanism was challenged by two famous judgments, *Gauweiler* (also known as *OMT*), and *Pringle*. On OMT, see in particular Takis Tridimas, and Napoleon Xanthoulis, "A Legal Analysis of the Gauweiler Case," in "The European Court of Justice, the European Central Bank and the Supremacy of EU Law," Federico Fabbrini, *Maastricht Journal of European & Comparative Law* , Special Issue 23, 1 (2016): 17-39, https://dx.doi.org/10.1177/1023263X1602300102.
See also "Peter Gauweiler and Others v Deutscher Bundestag, Case C-62/14," EUR-Lex**,** Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0062. Also "Thomas Pringle v Government of Ireland and Others, Case C-370/12," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0370.
[614] "Federal Republic of Germany v European Parliament and Council of the European Union, Case C-376/98," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A61998CJ0376 (*Tobacco Advertising I*); "Federal republic of Germany v European Parliament and Council of the European Union, Case C-380/03," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62003CJ0380 (*Tobacco Advertising II*). Stephen Weatherill, "The Limits of Legislative Harmonization Ten Years after Tobacco Advertising: How the Court's Case Law has become a 'Drafting Guide'," *German Law Journal* 12,3 (2011): 828.

regard to competences, the ones attributed to the EU are divided into exclusive competences[615], shared competences[616] and complementary or indirect competences[617]. In the event of uncertainty, the default option is that the competence is shared, and the EU can intervene first in order to regulate it (the effect is quite similar to the concept of American pre-emption[618]).

Bearing these elements in mind, an analysis of the liability competence produces the following results: liability is not explicitly mentioned either in the exclusive competences or complementary competences, hence it is shared. As a matter of fact, the EU has already had a chance to regulate liability with the PLD, but also had a chance in another important field which is that of environmental protection[619]. However, after the PLD there has not been another legislative act that has tackled the issues of private law liability directly in the MS. This is not to say that there were no efforts on the part of EU private law scholars to further harmonise the different private law liability regimes[620] but none apart from the PLD succeeded. This is because the competence, and eventual pre-emption/primacy[621] that the EU can exercise are limited by the principle of proportionality, set out in Article 5(4) TEU, which can be understood as a judicial exercise in assessing the necessity and the appropriateness of an EU action towards MS law or the rights of an individual[622].

---

[615] Articles 2 and 3 TFEU.
[616] Article 4(1). Marcus Klamert, "Article 4 TFEU," In *The EU Treaties and the Charter of Fundamental Rights*, Manuel Kellerbauer, Marcus Klamert and Jonathan Tomkin (Oxford: Oxford University Press, 2019), 35-60, https://dx.doi.org/10.1093/oso/9780198759393.003.7.
[617] Article 2(5) TFEU.
[618] See the subsection dedicated to medical devices cases in the US 2.3 in Chapter VI.
[619] "Directive 2004/35/CE of the European Parliament and of the Council of 21 April 2004 on environmental liability with regard to the prevention and remedying of environmental damage, OJ L 143, 30.4.2004, p. 56–75" EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32004L0035, Hereinafter Environmental Liability Directive or ELD.
[620] Among these pan-European efforts allow me to recall the Commission on European contract law otherwise known as the Ole Lando Commission (See section 1). Another effort involved the Principles of Tort Law the Principles of European Tort law. See European Group on Tort Law, *Principles of European Tort Law*, Accessed 31 January 2023, http://www.egtl.org/docs/PETL.pdf . Another milestone was the drafting of the Draft Common Frame of Reference. Study Group on a European Civil Code and the Research Group on Private Law (Acquis Group), *Draft Common Frame of Reference Draft Common Frame of Reference*. Munich: Sellier, 2009, https://www.law.kuleuven.be/personal/mstorme/2009_02_DCFR_OutlineEdition.pdf. The DCFR was considered by some as an EU private law civil code but in name, an optional instrument and by others as a complementary tool, a sand box for the EU Commission to take inspiration for future initiatives in contract law. For more discussion on the issue see Nils Jansen and Reinhard Zimmermann, " A EUROPEAN CIVIL CODE IN ALL BUT NAME": DISCUSSING THE NATURE AND PURPOSES OF THE DRAFT COMMON FRAME OF REFERENCE, *Cambridge Law Journal* 69,1 (2010): 98, https://dx.doi.org/10.1017/S000819731000019X.
[621] In particular, Arena maintains that while the primacy principle has been the one most often mentioned since the *Costa Enel Case*, the pre-emption doctrine is connected to it, but it has been more obscure and less analysed. In his opinion, while the principle of primacy is connected to the way in which conflicts between EU law and MS law must be solved, pre-emption doctrine instead concerns the time in which these conflicts are supposed to arise in non-exclusive competence areas. Arena, Amedeo. "The Twin Doctrines of Primacy and Pre-emption," In *Oxford Principles Of European Union Law: The European Union Legal Order: Volume I,* Robert Schütze and Takis Tridimas (Oxford: Oxford University Press, 2018), 322-349 https://dx.doi.org/10.1093/oso/9780199533770.003.0012.
[622] The most prominent reflections on the proportionality principle. See more in Takis Tridimas, "The Principle of Proportionality," In*Oxford Principles of European Union Law: The European Legal Order: Volume I*, Robert Schütze and Takis Tridimas (Oxford: Oxford University Press, 2018), 243-246, https://dx.doi.org/10.1093/oso/9780199533770.003.0010.

However, apart from proportionality, liability can also be connected to the constitutional traditions of the MS[623], making it a concept closer to a national than to a European level. Despite this closer national link, liability can truly become a more European concept thanks to a series of factors. Firstly, the judges of the CJEU belong to a specific legal system for many years before assuming that function. Secondly, it has been shown that even when discussing EU law, CJEU judges keep several legal models as references, relying on legal comparative methods when discussing and deciding cases[624]. Thirdly, the CJEU in particular has been a major cause of legal integration by relying on the dialogue with national courts, while at the same time applying the principle of procedural autonomy. This means that the CJEU formally refused to judge the substantial and procedural rules of the MS if they were not connected to EU law[625]. Nevertheless, it seems that the CJEU can investigate the respect of fundamental rights in the EU and evaluate how they are implemented in the MS[626]. In any case, it seems that with regard to the content of the many kinds of private law liabilities, MS are still free to also implement EU inputs in the digital field as they see fit[627].

Regarding private law, regulating private liability such as product liability might be less difficult than the regulation of criminal liability of technologies given that the PLD has been in place for more than 30 years and updating it is easier than drafting a brand-new liability directive.

2.2. Is Article 114 TFEU (harmonization) and the single market clause sufficient to establish liability for new technologies in general?

[623] Michele Graziadei and Riccardo De Caria, "THE « CONSTITUTIONAL TRADITIONS COMMON TO THE MEMBER STATES » IN THE CASE-LAW OF THE EUROPEAN COURT OF JUSTICE : JUDICIAL DIALOGUE AT ITS FINEST-estratto," *Rivista Trimestrale di Diritto Pubblico* 4 (2017): 949-971.
[624] Michele Graziadei, "The European Court of Justice at Work: Comparative Law on Stage Behind the Scenes," *Journal of Civil Law Studies* 13,1 (2020):8-14.
[625] Anthony Arnull, "Remedies Before National Courts," In *Oxford Principles Of European Union Law: The European Union Legal Order: Volume I*, Robert Schütze and Takis Tridimas (Oxford: Oxford University Press, 2018), 1012-1018, https://dx.doi.org/10.1093/oso/9780199533770.003.0036
[626] See the recent judgments according to which a conditionality mechanism based on human rights in order also to obtain financial subsidies from the EU is legal according to the EU. See "Hungary v European Parliament and Council of the European Union, Case C-156/21," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62021CJ0156. Also "Republic of Poland v European Parliament and Council of the European Union, Case C-157/21," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62021CJ0157. For a comment of the two judgments see Sarah Progin-Theuerkauf and Melanie Berger, "ECJ Confirms Validity of the Rule of Law Conditionality Regulation," *European Law Blog*, March, 11 2022, Accessed 31 January 2023, https://europeanlawblog.eu/2022/03/11/ecj-confirms-validity-of-the-rule-of-law-conditionality-regulation/.
[627] This is shown for instance in the diversity by the national implementation of the SDG and DSCD. See for more Alberto de Franceschi, "Country Reports: Italian Consumer Law after the Transposition of Directives (EU) 2019 / 770 and 2019 / 771," *Journal of European Consumer and Market Law 2*(2022):72-76; Jorge Morais Carvalho, " Country Reports: The Implementation of the EU Directives 2019/770 and 2019/771 in Portugal," *Journal of European Consumer and Market Law* 11,1(2022):31-34.

In this part of the subsection, the structure of Article 114 TFEU will be analysed and there will be some personal legal reflections on how it relates to the EU digital strategy.

Article 114 (formerly 110 TEC) TFEU, has been one of the main vectors of EU legal integration and has also been used as the main legal basis, even when the objective was consumer protection. A rapid overview of past legislative acts on EU consumer law will show that Article 114 TFEU on approximation appears most times compared to the consumer protection clause, which is Article 169 TFEU[628]. Its focus is the approximation of laws in order to obtain harmonization of MS legislations and a uniform effect to also achieve a high protection effect[629]. As already mentioned, some of the most important EU legal acts concerning consumer protection have been adopted on this basis, more so than using the clause that explicitly regulates consumer protection (Article 169) TFEU[630]. This can also be explained by the fact that, for many years, the EU adopted a neoliberal point of view[631]. Hence, instead of relying on a rights-based approach, the EU preferred the way of economic integration, which could be realised by the elimination of trade barriers[632]. Therefore, Article 114 TFEU and its predecessors on the approximation of laws in the common (and then single) market were considered an optimal tool to remove material and non-material barriers in order to fully exercise the four market freedoms. This process was supposed to have immediate consequences on economic integration, but also secondary consequences such as to ensure a higher level of protection for consumers and citizens in general, which is in any case one of the objectives of Article 114 TFEU[633].

MS have considered the frequent application of the harmonization clause (Article 114 TFEU) and the flexibility clause (Article 352 TFEU) as attempts by the EU and its predecessors to surreptitiously expand its competences[634]. It is true that Article 114 is general and is intended for a broad application, but it is not limitless: Article 114(2) TFEU expressly excludes some themes such as fiscal dispositions, matters in the free movement of people and rights and interests of employed persons. Moreover, each proposal that is based on Article 114 TFEU must provide a detailed plan of the costs concerning the initiative for which it is deemed the exact legal basis. Furthermore, Article 114 TFEU sets up a mechanism through which MS can object to new legislative initiatives founded on Article 114[635]. Finally, with its judgments, the CJEU has *de facto* drafted a guide

[628] Sacha Garben, "Article 169 TFEU," In *The EU Treaties and the Charter of Fundamental Rights: A Commentary*, Manuel Kellerbauer, Marcus Klamert and Jonathan Tomkin (Oxford University Press: Oxford, 2019), § 1460, https://dx.doi.org/10.1093/oso/9780198759393.003.280.
[629] Article 114(3) TFEU.
[630] Sacha Garben, " Article 169 TFEU."
[631] This neo-liberal approach was also used in the first period of Internet governance. Giovanni De Gregorio, "Digital Constitutionalism: An Introduction," In *Digital Constitutionalism in Europe*, Giovanni De Gregorio (Cambridge: Cambridge University Press, 2022):2, https://dx.doi.org/10.1017/9781009071215.002.
[632] "Digital Constitutionalism: An Introduction," In *Digital Constitutionalism in Europe*, Giovanni De Gregorio (Cambridge: Cambridge University Press, 2022):2, https://dx.doi.org/10.1017/9781009071215.002.
[633] Article 114(3) TFEU
[634] Craig- De Burca (2015), 92
[635] Article 114 (4),(5),(6),(7),(8),(9),(10) TFEU.

to apply the article to avoid criticism for "competences creep" over the years[636]: The *first Tobacco Advertising case* was the first time ever that an EU legal act had to be annulled as it suggested measures for the tobacco trade that contradicted the Internal Market principles, hence it was not proportionate[637]. Also, the sequel, the *Tobacco Advertising II case*, repeated the same principle; in *Vodafone*[638] it was also made it explicit that Article 114 TFEU had to be used "genuinely" to improve the functioning of the internal market and that "[…] *a mere finding of disparities between national rules and the abstract risk of infringements of fundamental freedoms or distortion of competition is not sufficient to justify the choices of Article 95 EC legal basis*" [639] and could not be used for all the internal market provisions.

The application limits of this clause are not only the explicit ones within the text of Article 114 TFEU, but also the ones of the EU legal order in general: hence the principles of proportionality and subsidiarity counteract the general application of Article 114 TFEU. In this respect, the CJEU has enforced the principle of proportionality more, as in *Digital Rights Ireland*[640].

Nevertheless, harmonization can happen in different ways: there can be minimum, maximum and partial harmonization. The names given to the first two types are rather self-explanatory and reveal the extent of the methods and the effects that the EU chooses in order to attain a more uniform approach on the subject. For instance, the SDG and DCDS are both explicitly pertaining to maximum harmonization[641], and the "black" list of unfair commercial practices (the ones which are always forbidden) are also maximum harmonization measures, as MS cannot set other standards or ways to achieve the same objective as the EU legislative act unless explicitly authorised to do so[642]. Conversely, minimum harmonization means that the EU leaves MS with leeway as they can set more exacting standards[643]. Partial harmonization instead is a

---

[636] Stephen Weatherill, "The Limits of Legislative Harmonization Ten Years after Tobacco Advertising : How the Court ' s Case Law has become a " Drafting Guide ","*German Law Journal* 12,3(2011) 828.
[637] "Federal Republic of Germany v European Parliament and Council of the European Union, Case C-376/98," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A61998CJ0376&qid=1675934963313. Hereinafter*, Tobacco I Advertising.* "Federal Republic of Germany v European Parliament and Council of the European Union, Case C-380/03,"EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62003CJ0380. Hereinafter *Tobacco Advertising II*.
[638] "The Queen, on the application of Vodafone Ltd and Others v Secretary of State for Business, Enterprise and Regulatory Reform, Case C-58/08," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62008CJ0058. Hereinafter *Vodafone*.
[639] §32 *Vodafone* Judgment.
[640] In this case, the CJEU had found out that the Data Retention directive needed to be annulled as the amount of time in which it was allowed to store personal data was considered disproportionate with the counterbalancing fundamental rights of privacy and data protection.
"Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, Cases C-293/12 and C-594/12," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293. Hereinafter *Digital Rights Ireland*.
[641] Articles 4 of both SDG and DCDS.
[642] Manuel Kellerbauer, "Article 114," In *The EU Treaties and the Charter of Fundamental Rights: A Commentary*, Manuel Kellerbauer, Marcus Klamert and Jonathan Tomkin (Oxford: Oxford University Press, 2019) https://dx.doi.org/10.1093/oso/9780198759393.003.280 1238.
[643] Kellerbauer, supra note, 1238

quality that can be attributed to a specific disposition that can coexist within a framework of minimum and maximum harmonization[644]. Further, harmonization can also be pursued indirectly: mutual recognition can also be used by the EU in certain disciplines[645] to obtain approximation of laws and standards.

Knowing that 114 TFEU is a general and flexible but not unlimited clause, it comes as no surprise that the Commission is founding its digital strategy on Article 114 TFEU. To be fair, for the sake of subsidiarity, the Socio Economic Committee and the Committee of Regions provided evaluations of some of the documents (such as the AI strategy) because of their widespread implications even if that is not requested by the ordinary legislative procedure[646]. It is also relevant that whenever personal data might be involved, the EDPB and the EDPS express opinions on the Commission's digital strategy proposals. This is due to the fact that it is partly established in their funding regulation but also, presumably, the Commission wants to make sure that the opinion of specialised bodies in data protection is heard before the legislative *iter* is completed. Moreover, all the proposals concerning the new digital strategy have a detailed financial plan and they also require the joint opinion of both the EDPS and the EDPB concerning the impact of the proposal on the actual data protection framework.

As mentioned before, however, both the reference to the principle of proportionality in connection with Article 114 TFEU's legal basis and technology is far from being fully explained. In particular, an objection could be made that the text of Article 114 TFEU does not make any reference to data whatsoever, and the relationship with the digital single market for data is not clear. As far as the memoranda seem to imply, the digital single market is a sub-category of the Internal Market that focuses more on data. This seems to be partly the case. The Data Act memorandum explicitly mentions an internal market for data[647]. Other proposals are less precise on this aspect and the focus is the danger of creating national rules that could either fragment the market or disrupt competition[648]. According to the *Vodafone* judgment, however, the justification to use Article 114 TFEU cannot be limited to the simple mention of disruption of competition and potential harm to fundamental rights. In all the proposals cited, the motivations

[644] For instance, in the SDG directive, the MS are free to set effective remedies that have to follow Article 13 indications but, at the same time, must be adapted to each of the MS legal contexts. Kellerbauer, supra note, 1238.
[645] Kellerbauer highlights, especially for the application of the freedom of movement of goods, Articles 34, 35, 36 TFEU, as established in *Brasserie du Pêcheur*, and its limits, in the *Keck* judgment." "Brasserie du Pêcheur SA v Bundesrepublik Deutschland and The Queen v Secretary of State for Transport, ex parte: Factortame Ltd and others, Cases C-46/93 and C-48/93," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A61993CJ0046. "Criminal proceedings against Bernard Keck and Daniel Mithouard. Cases C-267/91 and C-268/91," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A61991CJ0267.
[646] Article 294 TFEU.
[647] Proposal of the Data Act memorandum p.7 refers to an Internal Market for data.
[648] Proposal for the DMA refers to the fact that MS wanted to regulate the relationship between users and core platform service as a sign of fragmentation (p.4); in the DSA, the proper functioning of the Internal Market concerning cross border services is not explained and lays down harmonised conditions in the EU (p.5). The proposal for the regulation of AI states that there is a need for harmonised rules to prevent the fragmentation of the AI technology regulations (p.6).

that prevailed in the legal basis section (meaning the justification for the use of Article 114 TFEU) are not clearly detailed and were condensed into few lines of text.

That is why it is important to understand the relationship between "classic" "bricks and mortar" internal market harmonization and the digital single market one. If not made explicit, the CJEU must also expect judgments concerning the proportionality and subsidiarity principles and how they are respected by these acts, in addition to the legal basis issues. To date, the relationship between internal market and internal market for data is not explicit. One cannot justify the relationship of inclusion of the digital single market within the main internal/single market by relying on a literal interpretation of Article 114 TFEU as the terms "data" or "data protection" are never mentioned.

On the one hand, if data (including personal data) are implicitly included in the sphere of application of Article 114 TFEU, as they can at times be seen as services, and at times as goods (for instance some kinds of digital content), this means that they respond to the four fundamental freedoms of the treaties, hence the rules for a single internal market without trade barriers fully apply. This seems to be the interpretation of the Commission in the first Digital Single Market Strategy[649]. On the other hand, the view of data not solely as a commodity, seems to be more evident in the Shaping the EU Digital Future communication, where two out of the three objectives take into consideration people and democracy in the digital age[650]. This change of view on data as an enabler of fundamental rights is a process that is older than the last Commission communication. Especially after the introduction of the GDPR, processing data, especially if personal (we already know from Chapter III that the CJEU has an extensive interpretation of what personal data means), has become more difficult. In fact, it is the same GDPR that establishes the protection of the fundamental right to data protection as one of its legal bases and, complementary to that, a risk-management approach in order to avoid fundamental rights infringement and ensure the free circulation of data[651].

The analysis of CJEU jurisprudence can shed some light on the relationship between the internal and digital single market. The single/ internal market case law witnessed the progressive recognition of human rights, but even in recent times, social rights had to be reduced in favour of the freedom of establishment and the provisions of services, such as in the *Viking* and *Laval* cases[652]. As far as the digital single market is concerned, there is a stark

[649] "COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A Digital Single Market Strategy for Europe, COM/2015/0192 final," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192, 3.
[650] "COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Shaping Europe's digital future, COM/2020/67 final," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52020DC0067, 2.
[651] Recitals 1 and 2 of the GDPR.
[652] "International Transport Workers' Federation and Finnish Seamen's Union v Viking Line ABP and OÜ Viking Line Eesti, Case C-438/05," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-

distinction between competition-intellectual property cases and data protection-fundamental rights ones. It is particularly apparent that the ambivalence of data, which can simultaneously be a human right enabler and a commodity, is going to characterise digital single market development, a quality that was not as evident with the previous single-internal market, with the notable exception of the freedom of movement of people.

2.3. The Charter for Digital Rights and a progressive path towards a more Constitution-oriented legal integration of new technologies

The digital single market is more connected than its predecessor to the fundamental rights dimension. This also happens because new technologies, and in particular the IoT - also for domestic use - are silent and pervasive technologies which rely on personal and non-personal data that they intercept from us, whether we are aware of the fact we are sharing data or not. It is not surprising, then, that the Commission published Digital Rights and Principles for the Digital Decade on 26 January 2022[653].

One can understand the reasons concerning the timing and the rationale of this communication just by considering the context of the pandemic. Since February 2020, various forms of technologies (which were once rarely used) have become widespread in EU citizens' everyday life: from contact-tracing apps to video-conferencing tools. Two factors have become more apparent: the first factor is that there is an increasingly common belief that there must be specific rights for the digital society, even though they are not always easy to identify[654]. This could be understood with the fact that the boundaries between the digital and the physical worlds are becoming ever more blurred[655]. The second factor is that power is now not only exercised by public authorities, at a national or transnational level, but also by other private and global actors such as platforms or search engines, which wield significant economic and infrastructural power[656]. Generally, these groups of subjects have become a core part of the Internet structure at large, and are able to wield access to digital markets and

content/EN/TXT/?uri=CELEX%3A62005CJ0438. "Laval un Partneri Ltd v Svenska Byggnadsarbetareförbundet, Svenska Byggnadsarbetareförbundets avdelning, Byggettan and Svenska Elektrikerförbundet , Case C-341/05," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62005CJ0341. For a commentary Norbert Reich, "Free Movement v. Social Rights in an Enlarged Union - the Laval and Viking Cases before the ECJ," *German Law Journal* 9,2(2008): 125-161.

[653] "European Declaration on the Digital Rights and Principles for the Digital Decade. COM/2022/28 final," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A28%3AFIN. Hereinafter, Charter for Digital Rights.

[654] Bart Custers, "New digital rights: Imagining additional fundamental rights for the digital era," *Computer Law and Security Review* 44(2022):10536, https://dx.doi.org/10.1016/j.clsr.2021.105636.

[655] The Onlife Initiative, "The Onlife Manifesto," In *The Onlife Manifesto: Being Human in a Hyperconnected Era*, Luciano Floridi (Cham, Switzerland: Springer 2015), 1-13.

[656] Giovanni De Gregorio, "The Law of Platforms," In *Digital Constitutionalism in Europe*, Giovanni De Gregorio (Cambridge: Cambridge University Press, 2022), 80-122. https://dx.doi.org/10.1017/9781009071215.004.

communities, also due to the fact that they own such large quantities of data (of any kind) making it impossible to be their competitors.

The response of EU regulators to this state of matters is two-fold. On the one hand, within the framework of a strategy, there is the need to develop a digital single market connected to a digital society, and to suggest legal acts that can deal with different technological phenomena in the most coherent way possible. On the other hand, probably following input from a novel digital constitutionalism[657], the EU regulators can decide to establish principles and rights concerning technology. Ultimately, these can influence both the law and technology in the interest of preserving democratic societies, both online and offline. The new Declaration would appear to respond to this second motivation. These rationales underpin the first paragraph of the preamble of the European Declaration on Digital Rights and Principles for the Digital Decade, which was solemnly proclaimed by the three main institutions: the European Parliament, the Council and the Commission[658]. Despite that, the Charter currently has solely a declaratory nature[659], hence it is not mandatory.

Despite not being currently obligatory in character, it is interesting to notice that, in the context of the digital transition, the Charter's set of rights and principles must become a reference for all the stakeholders in general, therefore both for actors within the EU ad outside the EU[660]. Even though there is no express reference to liability for new technologies in any of the six chapters of this declaration, some elements are worth mentioning. Firstly, there is still an emphasis on the person as the filter through which the digital revolution must happen. In liability terms, it means that there will be no excuse for the damage that might be caused by semi-autonomous machines, such as some kinds of domestic IoT[661]. Secondly, a right to connectivity in the second chapter is developed in two ways: on the one hand, the right to be online has become a fundamental right, as theorised by Rodotà[662]; on the other hand, there is the defence of a neutral internet where there are no blocks of services and content. This is interesting when considered in relation to the application of the two directives SDG and DCDS. If this declaration is to become mandatory, the legal obligations of the traders and sellers will not only be grounded on national conceptions of contractual good faith, but they will also have to comply with technology neutrality principles. Thirdly, in relation to the IoT, chapter V of the Charter is relevant in establishing that all technologies must be privacy-protective by design. Hopefully, this could also influence third country importers of domestic IoT within the EU. Moreover, the concept of user control of data is again

[657] Giovanni De Gregorio, "Digital Constitutionalism: The Law of Platforms," in Giovanni De Gregorio *Digital Constitutionalism in Europe*, (Cambridge: Cambridge University Press, 2022):80-122.
[658] Charter for Digital Rights, 1.
[659] Charter for Digital Rights, 1.
[660] Charter for Digital Rights, Preamble, Para 5, p.1
[661] Especially "fostering responsible and diligent action by all digital actors, public and private, for a safe and secure digital environment", Chapter I Charter for Digital Rights.
[662] Stefano Rodotà, "Dichiarazione dei Diritti di Internet," Camera dei Deputati, Accessed 31 January 2023, https://www.camera.it/application/xmanager/projects/leg17/commissione_internet/dichiarazione_dei_diritti_internet_pubblicata.pdf.

explained[663]. Finally, chapter VI insists on the environmental sustainability of technology. In terms of IoT design, this could determine further investments in the Green IoT and incentives to recycle, repair and re-use technological objects and components.

Nevertheless, the relationship between this Digital Rights Charter and the Treaty of Lisbon is still unclear. In fact, the Treaty belongs to the early days of digital societies and lacks effective instruments on how to handle present-day digital phenomena. One element might clarify this situation. The fact that the three main institutions decided to make this joint declaration is not a unique event in EU history and may have a precise meaning. The Declaration of Nice in 2000, which is now known as the Charter of Fundamental Rights and Freedoms of the EU, was solemnly proclaimed (as was the Charter on Digital Rights) by the three main EU institutions in Nice. Initially, the Charter of Fundamental Rights had a solely declaratory function, such as the one that the Charter on Digital Rights has today. In time, the Charter of Fundamental Rights that was solemnly declared in Nice became mandatory (Article 6 TEU) even though it does not reside within the Treaty[664]. The Charter united both the legal scholars' advancements in human rights theory and the fundamental rights recognised by the CJEU up to that moment. Similarly, this new declaration on Digital Rights can be the beginning of a new process to draft a new treaty for the EU, which will provide a better legal basis for the digital and environmental challenges of today and tomorrow. It is definitely too early to tell whether this hypothesis is correct, but the illustrious precedent of the Nice declaration provides some optimism.

3. Product Liability for the home IoT: which possible constitutional scenarios?

In brief, the digital single market is structurally different from the internal market, as fundamental rights and economic issues are intermingled within it. Due to its generality, Article 114 TFEU could still be employed for a future PLD. However, as the proposed Charter for Digital Rights also suggests, there will be a growing focus on how new technologies, including the IoT for the home, will impact on the citizens' autonomy and fundamental rights in general. Therefore, I believe that the current phase is a transitional one and that it precedes a reform of the Treaties to make them more suited to the digital age. It may be that the Charter of Digital Rights becomes mandatory as was the case with the Charter of Fundamental Rights and Freedom in the past. The optimal legal basis for a new PLD hypothesis would be an upgraded Article 114 TFEU, with the additional mention of the digital single market in addition to the internal market clause. This would enhance the respect of the digital single market's particular characteristics, the most significant one being the fact that the economic and human rights

[663] Charter for Digital Rights,5.
[664] Some MS decided to opt out such as Denmark and the UK.

dimension will always be relevant and will frequently require evaluation at the same time.

Chapter V: Towards an updated PLD for the domestic IoEd objects

Chapter V: Towards an updated PLD for the domestic IoEd objects ... 134
1. Introduction ... 134
1.1. The PLD: history and legal models ... 135
1.1.1. European Product Liability models before the EU PLD ... 139
1.1.2. EU PLD between: the US model and EU harmonization ... 141
2. The implementation of the PLD: a quantitative and qualitative study based on the case law of the CJEU ... 142
2.1. First quantitative and qualitative analysis of EU PLD related cases: number and types of cases per Member State. ... 158
2.2. Second quantitative and qualitative analysis: the EU PLD most challenged articles ... 163
3. The future PLD and its interaction with other legislative and policy documents. ... 170
3.1.1. Future Article 2 PLD ... 171
3.1.2. Future Article 3 PLD ... 174
3.1.3. Future Article 4 PLD ... 177
3.1.4. Future Article 6 PLD ... 178
3.1.5. Future Article 7 PLD ... 180
3.1.6. Future Article 9 PLD ... 182
3.1.7. Future Article 11 PLD ... 187
3.1.8. Future Article 13 PLD ... 188
4. Preliminary conclusions ... 190

1. Introduction

This chapter focuses on one of the EU legislative acts that will probably still be applied whenever an IoT for the home is involved. Moreover, it is the EU Consumer *acquis* legislative act that has not yet been updated by the EU Digital Strategy policy: the Product Liability Directive (PLD)[665]. My intention is to discuss whether the rationales and contingent events that led to the drafting of the current PLD text are still fit to be applied to the home IoT technology. I will therefore analyse which models existed and which ones still exist in the EU concerning product liability that are different from the EU law regime (1.1.1).I will then list the most important opinions in the debate on the functions of the PLD directive (1.1.2). Thereafter, I will analyse the corpus of judgments that concern the application of the product liability directive in the CJEU jurisprudence, both from a quantitative and qualitative point of view (2). The purpose of this analysis is

[665] "Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products *OJ L 210, 7.8.1985, p. 29–33,"* EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31985L0374.

two-fold. The first is to discover which articles of the PLD were most challenged. This serves to find out whether the current regime of the PLD or national models were found to be efficient in tackling problems with connected domestic objects. The second purpose of this kind of analysis is that knowing which articles were challenged the most could also help to clarify how the PLD should be updated to make it more adapted to new technological risks. In addition, the study of the CJEU judgments on the PLD allows to understand the points of friction or overlap that the PLD discipline may have with other EU legislative acts or proposed legislative acts concerning technologies. This might be useful in a perspective analysis of damages that could be caused by the data processing techniques used by the domestic IoT object. The final part of the chapter discusses whether it is already possible to provide inputs and suggestions for the redrafting of those articles of the PLD that have been most often challenged before the CJEU, to adapt them to the challenges which arise from the use and deployment of IoT technology for the home (3).

1.1. The PLD: history and legal models

One of the results of Chapter III was that the PLD was perhaps one of the most important legislative acts in the area of *consumer acquis* that had not been the subject of a formal European Commission policy proposal concerning its Digital Strategy. Nevertheless, the PLD's adaptability to new technologies has been tested by EU policy makers for quite some time. The 2018 REFIT fitness check of EU consumer law, which scrutinised the entire consumer law *corpus*, considered the PLD [666] still fit for purpose[667] when applied to new technologies. European legal scholars criticised this result because the methodology used to carry out this assessment, combined with quite an ambitious expected research result, was applied for a limited period of time to obtain such clear results[668]. Already two years after the launch of the Digital Single Market strategy, EU legal scholarship agreed that it was time to re-think EU consumer law in a more solid and innovative way than in the past[669]. Nowadays the majority of legal scholars believe that an amendment to the PLD is required, especially when it comes to new technologies such as the IoT, robotics and AI, although a common understanding about the extent of this reform is still not forthcoming[670]. That is

[666] "REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL AND THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE on the Application of the Council Directive on the approximation of the laws, regulations, and administrative provisions of the Member States concerning liability for defective products (85/374/EEC) COM/2018/246 final," 2, EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52018DC0246.
[667] REFIT Scoreboard, Accessed 31 January 2023, https://op.europa.eu/webpub/com/refit-scoreboard/en/policy/11/index.html.
[668] Aurelia Colombi Ciacchi et al., "Position Paper on the Fitness Check of EU Consumer Law," *European Review of Private Law* 26,5(2018): 703-706.
[669] Christian Twigg-Flesner, "From REFIT to a rethink: time for fundamental EU Consumer Law reform," *Journal of European Consumer and Market Law* 6(2017):185-189.
[670] The extent of the update then depends on the personal views of the scholars on the matter, who are almost always influenced by the legal system they live in. For instance, Professor Christiane Wenderhorst is in favour of changes in order to update the PLD in a way not to cause more legal disruption than necessary; Professor Bernard A. Koch agrees with this view, to mention only two scholars based in

also why there are two functioning European Product Liability Formations study groups, funded by the Commission in 2018. Their tasks are differentiated: the first must evaluate the fitness of the PLD in light of the impact of digital technologies on product liability, while the second focuses instead on the impact of new technologies on liability in general. The Expert Group on Liability for AI and new technologies was mentioned in Chapter III due to its report on the liability of AI and new technologies[671] and it deals, not surprisingly, with the impact of AI also on strict liability regimes such as the PLD. In recent years, prominent associations of EU independent scholars such as the European Law Institute (ELI) and autonomous researchers have shared their ideas on the structure and contents of a possible PLD fit for new technologies, which will most likely include domestic IoT objects. In order to better understand how IoT technology for the home will impact with the actual text of the PLD, I will schematically go through the main contents of the PLD that is the document of EU consumer law *acquis communautaire* which has survived the longest and with minimal amendments[672]. In this way, it will be easier to understand the references to the articles of that text in the quantitative and qualitative study found in paragraph 2.1 and 2.2.

The PLD was the legislative act that started the New Approach. Practically, this means that the Commission sets parameters and the MS and private stakeholders implement them[673], in order to promote a better governance model. The New Approach was the "ancestor" of the actual New Legislative

Austria. Conversely, Professor Giovanni Comandè suggests a more innovative approach by considering blending the concept of liability and accountability for AI (if one has a wide definition of AI also the IoT as cloud base system is comprehended), while Professor Georg Borges predicts an increased use of insurance and compensation funds used in more creative way as instruments to reduce new technologies risks. Christiane Wendehorst, "Strict Liability for AI and other Emerging Technologies," *Journal of European Tort Law* 11,2(2020): 178, https://dx.doi.org/10.1515/jetl-2020-0140. Bernhard A Koch, "Product Liability 2.0- Mere Update or New Version?," in *Liability for Artificial Intelligence and the Internet of Things. Münster Colloquia on EU Law and the Digital Economy,* Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (Baden Baden: Nomos Verlag- Hart Publishing, 2019), 115-116. Georg Borges, "New Liability Concepts: the Potential of Insurance and Compensation Funds," in, *Liability for Artificial Intelligence and the Internet of Things. Münster Colloquia on EU Law and the Digital Economy,* Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (Baden Baden: Nomos Verlag- Hart Publishing, 2019),145-163. Giovanni Comandè "Multilayered (Accountable) Liability for Artificial Intelligence," in, *Liability for Artificial Intelligence and the Internet of Things. Münster Colloquia on EU Law and the Digital Economy,* Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (Baden Baden: Nomos Verlag- Hart Publishing, 2019),165-183.

[671] Expert Group on Liability and New Technologies, *Liability for Artificial Intelligence Report from the Expert Group on Liability and New Technologies-New Technologies Formation* (Brussels: European Commission, 2019), Accessed 31 January 2023, https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608. I have already partially assessed this in Chapter III and IV as far as its value of an influential policy instrument although some of its proposals have been criticised by other scholars, notably Professors Bertolini and Episcopo. See Andrea Bertolini and Francesca Episcopo, "The Expert Group's Report on Liability for Artificial Intelligence and Other Emerging Technologies: A critical assessment," *European Journal of Risk Regulation* 12,3 (2021): 644-659 https://dx.doi.org/10.1017/err.2021.30. In this chapter, the content of this report will be recalled each time there is a description between the traditional PLD concept and domestic IoT but the main focus would be how its principles will apply to domestic technology.

[672] Daily Wuyts, "The Product Liability Directive- More than two Decades of Defective Products in Europe," *Journal of European Tort Law* 5,1 (2014):1-3, https://dx.doi.org/10.1515/jetl-2014-0001.

[673] Anna Wallerman, "Pie in the sky when you die? Civil liability of notified bodies under the Medical Devices Directive: *Schmitt*," *Common Market Law Review* 55(2018):265.

Framework[674], which strives to create an even better system of governance and involvement of all the stakeholders in certain decisional processes, especially the ones concerning technical subjects such as standards (see Chapter II and IV). The PLD's main principle is in Article 1, which states that the producer is the main subject who is responsible for the damage caused by the product[675]. However, in order not to leave loopholes, there is also a series of other subjects that could be considered as if they were the producer whenever the producer cannot be reached, or its identity is not known. In fact, one can consider a subject as a producer if they present themselves as such by using the producer's distinctive signs. In addition to that, the importer and the supplier could also be considered as producers[676].

The PLD also gives criteria for the division of the compensation if damage is caused by a plurality of subjects. Article 5 PLD adds that when several subjects are responsible for the same damage, they will be held liable jointly and severally, without prejudice to the applicable national law on the issue.

With regard to the field of application, the PLD concerns all movable products, even if incorporated into other objects. Agricultural products and electricity are expressly included[677]. As already mentioned in chapter IV, the PLD introduces a form of strict liability but with some requirements. The injured party is not obliged to prove any fault on the producer's side but needs to provide evidence concerning the product's defect, the damage caused and the causal relationship linking the defect of the product with the damage endured[678]. Regarding the elements that the plaintiff has to prove, the PLD contains a rather general notion of defect. Article 6(1) PLD states that a product is defective "[…] *when it does not provide the safety which a person is entitled to expect*". It continues by indicating some ways in which a product can be considered defective. The lack of safety can be determined by the presentation of the product[679], by its use[680] and the time in which it was placed in circulation[681]. This list is quite general and covers several situations. Article 6(2) PLD also specifies that a product is not defective if a newer and better version is subsequently marketed. The reference to the safety that a person can expect is inspired by the so-called consumer expectation test set forth in the Second Restatement of Torts in the US[682]. Nowadays, instead, in the US the product liability approach to evaluation of the defect and damage of a consumer product is based on the risk-utility test[683].

---

[674] "New legislative framework," European Commission, https://ec.europa.eu/growth/single-market/goods/new-legislative-framework_en, Accessed 31 January 2023.
[675] Article 1 PLD.
[676] Article 3(1),(2),(3) PLD.
[677] Article 2 PLD.
[678] Article 4 PLD.
[679] 6(1)(a) PLD.
[680] 6(1)(b) PLD.
[681] 6(1) (c) PLD.
[682] Jean-Sébastien Borghetti, Marta Santos Silva et al., "Relevance of risk-benefit for assessing defectiveness of a product: A comparative study of thirteen European legal systems," *European Private Law Review* 29,1(2021):93.
[683] Jean- Sébastien Borghetti, Marta Santos Silva et al., "Relevance of risk-benefit for assessing defectiveness of a product: A comparative study of thirteen European legal systems," *European Private Law Review* 29,1(2021):91-132; Mathias Reimann, "Liability for Defective Products at the beginning of the

Despite the fact that the PLD belongs to the "strict liability family", no kind of damage is subject to compensation under this regime, even if all the conditions of Article 4 PLD are met. Death or physical injuries are to be compensated[684] but compensation is also awarded for economic damage to an item of property[685]. For this subcase, there are two extra conditions. Firstly, the loss must be equivalent to the sum of 500 ecu (now euros) or more. Secondly, this item can be either of a type that is intended for private use or consumption[686] or was used by the injured person mainly for their own private use or consumption[687]. Moreover, the PLD allows the producer to have justifications if their products cause damage as described and proved. Producers can defend themselves if the injured person has fulfilled the conditions set by Article 4 PLD by demonstrating that their actions (or lack of) fall into one of the six exemptions of Article 7 PLD. The first exemption covers the case in which the product was not placed in circulation in the market by the producer[688]. The second one excludes liability when the defect which caused the damage did not exist at the time when the product was placed in circulation[689]. The third exemption states that the producer is not liable if it proves that the product was not manufactured by its company[690]. The fourth one concerns defects which are the consequence of mandatory regulations issued by public authorities[691]. The fifth exemption is called the risk-development exemption: it means that the producers cannot be held liable for any defect of the product which was not known in light of the scientific and technical knowledge at the time when the product was marketed[692]. The last exemption concerns the manufacturer of the object component if it succeeds in demonstrating that the defect is attributable to the design of the object[693].

The PLD also sets rules concerning how long the producers' liability lasts. Article 10 PLD establishes that producers' liability lasts for three years only, starting from the day on which the plaintiff became aware or should have reasonably become aware of the damage, defect and identity of the producer. However, Article 11 generally establishes a limitation period of ten years starting from the date on which the product is marketed. MS are in any case free to regulate the rules concerning the interruption and suspension of this period[694]. Finally, Article 13 PLD concerns the relationship of the product liability regime with other national sets of liability rules. This article actually states that the PLD "[…] *does not affect any rights which an injured person may have according to*

Twenty First Century: Emergence of a Worldwide standard?," *The American Journal of Comparative* Law 51,4(2003):751-838, https://www.jstor.org/stable/3649130.

[684] Article 9(a) PLD.
[685] Article 9(b) PLD.
[686] Article 9(b)(i) PLD.
[687] Article 9(b)(ii) PLD.
[688] 7(a)PLD.
[689] 7(b) PLD.
[690] 7(c) PLD.
[691] 7(d) PLD.
[692] 7(e) PLD.
[693] 7(f) PLD.
[694] 10(2) PLD.

the rules of the law of contractual or non-contractual liability". Both citizens and Member States (MS) challenged Article 13 PLD several times, not only through the preliminary reference procedure of Article 267 TFEU and in the course of infringement proceedings [695].

In order to better understand the extent of the change that is required, it is important to summarise the events that led to the approval of this directive and from which legal models inspiration was drawn or rejected.

1.1.1. European product liability models before the EU PLD

The PLD was not created in a legal void. At the end of the 20th century, product liability was indeed seen as a worldwide phenomenon (although with different standards) which needed to be tackled as a consequence of the large scale of contemporary industrialisation[696]. Europe[697], the US and North America in general were the first countries to feel the necessity to regulate the protection of weak parties and allow trade and commerce to flourish at the same time.

From a comparative and also future policy point of view, it is interesting to analyse some of the models that were used to deal with product liability issues before the European directive for two reasons. The first reason is that these legal models are part of each MS legal tradition and have also influenced the subsequent implementation of the PLD (when applicable) and case law directed to the CJEU. The second reason is that these models have frequently coexisted up to now alongside the PLD and sometimes are more protective of consumers than the PLD itself.

The first model is represented by those countries that extensively applied the warranties connected to the contract of sale prior to the PLD. France is the most representative of this group. France extensively applied its *garantie des vices cachés*, the contractual warranty system, not only towards the seller, but also toward suppliers. Former Article 1382 of the French civil code (now 1240) – the general provision on extra-contractual liability – was interpreted extensively when there was no contractual obligation between the plaintiff and the defendant[698]. This model is remarkably similar to the original remedies used for the development of US product liability, which will be examined in Chapter VI[699].

---

[695] See section 2 of this chapter.

[696] [696] Mathias Reimann, "Liability for Defective Products at the beginning of the Twenty First Century: Emergence of a Worldwide standard?," *The American Journal of Comparative* Law 51,4(2003):768, https://www.jstor.org/stable/3649130.

[697] Let us not forget that before the EU, the Council of Europe promoted a Convention on product liability in the event of damages to the person or death. Conseil de l'Europe, *Convention européenne sur la responsabilté du fait des produits en cas de lésions corporelles ou de décès*, Strasbourg, 27 January 1977, Accessed 31 January 2023, https://rm.coe.int/1680077328.

[698] Jean-Sébastien Borghetti, "Product Liability in France," in Piotr Machnikowski *European Product Liability: An Analysis of the State of the Art in the Era of New Technologies* (Cambridge, Portland Antwerp: Intersentia, 2016), 206-211.

[699] Michel Cannarsa, *LA RESPONSABILITÉ DU FAIT DES PRODUITS DÉFECTUEUX. ÉTUDE COMPARATIVE,* (Milano: Giuffrè, 2005), 19-86.

The second model to consider, for which we could take both Italy and Spain as examples, consists of countries in which product liability claims were at first adjudicated on the basis of contractual liability and judges and practitioners later preferred to enforce claims based on extra-contractual liability. Most countries representing this second model at first applied contractual liability rules that were typical of the sale contract, while disregarding or loosening the rules on the privity of contract. For instance, prior to the PLD, in Italy the rules on extra-contractual and fault liability were elaborated by legal scholars, then methodically applied in a balanced way by the judiciary[700]. At the beginning, however, Italy in some cases applied the rules of contractual liability, thus making an exception to the rule of the relativity of the effects of contract, or it used pre-contractual liability (which for an authoritative part of Italian legal experts has a contractual nature[701]). This dialogue between scholars and the judiciary also continued when the PLD began to be applied[702]. Before implementation of the directive, Spain, as well as Italy, had two kinds of actions, one based on contractual liability which lasted until the '70s. This was then substituted by the rules on general tort law[703]. The third model instead consistently relied on forms of tort liability to govern product liability claims, even prior to the PLD[704]. Germany applied its tort law principles for defective products with a reversal of the burden of proof with the case *Hünerpest*, in 1968[705]. For some, even nowadays the modern German law of torts applicable to product liability is not only more favourable than the PLD but also in some respects bears a resemblance to the solutions developed by the American Third Restatement of Torts[706]. The UK too implemented a specific action in tort based

[700] Eleonora Rajneri, "Country Reports: Product Liability in Italy," *Journal of European Consumer and Market Law* 5(2019): 209. However, the application of tort law was the ending part of a longer process which started by trying to apply extensively the sales warranties but also pre-contractual liability theories.
[701] For the developments of Italian legal scholars' reflections on product liability see Giovanni Comandè, "Product Liability in Italy," in Piotr Machnikowski *European Product Liability: An Analysis of the State of the Art in the Era of New Technologies* (Cambridge, Portland Antwerp: Intersentia, 2016),276-309.
[702] Eleonora Rajneri, "Country Reports: Product Liability in Italy," *Journal of European Consumer and Market Law* 5(2019): 209.
[703] Miquel-Martín Casals and Josep Solé Feliu, "Product Liability in Spain," in Piotr Machnikowski *European Product Liability: An Analysis of the State of the Art in the Era of New Technologies* (Cambridge, Portland Antwerp: Intersentia, 2016):408-411.
[704] This is not to exclude the existence of theories concerning contractual or quasi contractual solutions for product liability –like cases in Germany, but it was only in 1968, with the judgment *Hünerpest*, that the German Supreme Court ruled that tort needed to be the kind of liability to apply in these cases and, for the first time, it called them "product liability cases". On the contractual and quasi contractual theories present in German law before the *Hünerpest* case, see B.S. Markesinis, *The German Law of Obligations. Volume II. The Law of Torts: A comparative introduction* (Oxford: Clarendon Press, 1997), 83-89.
[705] Ulrich Magnus, "Product Liability in Germany", in *European Product Liability: An Analysis of the State of the Art in the Era of New Technologies*, Piotr Machnikowski (Cambridge, Portland Antwerp: Intersentia, 2016), 238-240.
[706] As a matter of fact, Stefan Lenze explained that the economic reasoning underpinning this comparison is that the German scholars and judiciary authorities judge the defectiveness by using a risk-utility reasoning. In short, the *"…intensity of the duty of care depends on the magnitude and on the foreseeability of risks of harm… in other terms the manufacturer is negligent if the increased (marginal) costs of the untaken safety precaution would have been less than expected damages"*. Judges and legal scholars have distinguished several kinds of duties of the producer and corresponding defects, such as manufacturing, design and warning duties. See Stefan Lenze, "German product liability: between European directives, American Restatements and common sense," in Duncan Fairgrieve (ed.) *Product Liability in Comparative Perspective*, (Cambridge: Cambridge University Press, 2005): 102-103. These are very similar to reasoning existing under the restatement third of torts. Also on the issue of the development of the evaluation of defects in traditional German product liability see Basil S. Markesinis, *The German Law of*

on a duty of care which was successful for the first time in the seminal case *Donoghue v. Stevenson*[707]. Strangely, in the UK, even before implementation of the PLD, there were not as many cases concerning defective products as those occurring in other countries (such as the US or France, see infra). Midway between the Italian-Spanish, German and the UK model, Denmark applied principles of judge-made tort law: the most important remedy in this respect was to apply the concept of vicarious liability to the suppliers of the product, who were considered in a better position to influence and legally challenge the producers[708].

1.1.2. EU PLD: the US model and EU harmonization

The model introduced by the PLD based on strict liability for damage caused by consumers' objects is apparently inspired by the American Second Restatement of Torts, but, in the end, it introduces rules that do not find an equivalent in the American legislation and case law. In fact, it would be incorrect to consider the PLD as a European equivalent of the American Restatement[709]. Whether the PLD was a harmonization measure (Art. 110 TEC now 114 TFEU) or a consumer protection policy measure (then 153 EC, now Art. 169 TFEU) was a matter of controversy for a time[710]. The solution, formally, is that it is a measure to build the Internal Market, hence it would now correspond to Article 114 TFEU. It cannot be said that it is more favourable to consumers *per se*, as the text itself is full of checks and balances in order to have balanced rules which also take the interests of producers into consideration. As will be explained infra, even EU case law on the PLD cannot be defined pro-consumer *in toto*. This can also be understood from its first two recitals. In particular the first states that there is no better instrument to regulate product liability than "[…] *approximation of the laws of the Member States concerning the liability of the producer for damage caused by the defectiveness of his products* [because otherwise…] *the existing divergences may distort competition and affect the movement of goods within the common market and entail a differing degree of protection of the consumer against damage caused by a defective product to his health or property*"[711].

Furthermore, a careful analysis of the PLD articles suggests that a balanced approach was sought by the drafters: it is true that it is (at least formally) easier for consumers to prove the damage (Article 4 PLD) compared to national standards of proof on tort liability, as the list of subjects that are potentially

Obligations. Volume II. The Law of Torts: A comparative introduction (Oxford: Clarendon Press, 1997), 90-95.

[707] Ken Oliphant and Vanessa Wilcox, "Product Liability in England and Wales," in in Piotr Machnikowski *European Product Liability: An Analysis of the State of the Art in the Era of New Technologies* (Cambridge, Portland Antwerp: Intersentia, 2016):174. Edween Peel and James Goudkamp, *Winifield Jolowicz Tort* (London: Thomson Reuters-Sweet&Maxwell, 2014, 19th ed.)1-008, 5-005.

[708] Marie-Louise Holle and Peter Møgelvang-Hansen, "Product Liability in Denmark," in Piotr Machnikowski *European Product Liability: An Analysis of the State of the Art in the Era of New Technologies* (Cambridge, Portland Antwerp: Intersentia, 2016):155-156.

[709] Marta Santos Silva et al., "Relevance of risk-benefit for assessing defectiveness of a product: A comparative study of thirteen European legal systems," *European Private Law Review* 29,1(2021): 91-132.

[710] Thomas Verheyen, "Full Harmonization, Consumer Protection and Products Liability: A Fresh Reading of the Case Law of the ECJ," *European Private Law Review* 26(2018): 137-139.

[711] First recital PLD.

assimilated to producers is a long one (Article 3), the notion of defect of Article 6(1) PLD is not rigid and Article 13 PLD clarifies that this Directive does not limit the pre-existent rights of consumers under previous contractual or non-contractual liability schemes. However, all these rules were interpreted quite strictly at the beginning of the 2000s due to the need to affirm that this was a maximum harmonization directive (more infra). Several other elements are also clearly in favour of producers: in fact, Article 7 PLD provides six liability exemptions. Moreover, the list of product defects considered as not meeting the consumer's expected level of safety does not extend to the fact that a more recent model of the same object can perform better than the old one (Article 6 PLD) and, finally, the recovery of damage in Article 9 PLD is not unlimited, especially with reference to property damage (there is a monetary cap plus the requirements of letter b of the same article).

The CJEU almost always framed the interpretation of the rationale of the directive in terms of a "delicate balance between different interests" that served the creation of the Internal Market. In particular, an extensive explanation on why the balance of the different interests needed to be considered was provided by AG Geelhoed[712] (see infra subparagraph 2.2). The AG, whose opinion was then adopted by the Court, made the point that the adoption of the Directive on product liability at the (then) European Community took almost twenty years. Such a lengthy process was motivated by the need to balance the reasons of consumers and producers, which were both instrumental in the creation of the Internal Market. If the PLD is indeed going to be updated, it is uncertain whether Article 114 TFEU on the harmonization of the Internal Market will continue to be the legal basis of the PLD. As already explained in Chapter IV, it would be more correct to have an updated version of Article 114 TFEU which explicitly includes the Digital Single Market reference. In this way, both fundamental rights and regulatory functions would be safeguarded. Moreover, this would also be coherent with the recently declared Charter of Digital Rights[713].

2. The implementation of the PLD: a quantitative and qualitative study based on CJEU case law

In order to reach the goal of this chapter, which is to identify, if any, the points that need to be changed in the PLD in order to make it compliant for new technologies, it is necessary to analyse the (nowadays) abundant CJEU case law that concerns the PLD. This is important also in order to assess:

a) which articles of the PLD were mostly litigated;
b) indirectly, which national legal liability models clashed the most with the rationale of the PLD and why;

[712] §35 and following of the Joined Opinion about the cases *Medecina Asturiana and France v Commission* Cases C-52/00 and C-183/00.
[713] See Chapter IV, subsection 2.3.

c) whether these points will also be relevant for the updating of the PLD which is necessary to meet the challenged posed by new technologies.

I will briefly outline the methodology used. As for the database, I used the EUR-LEX[714] website, and, in particular, the refined research in the case law subdomain. I decided to limit the dates from the 01/01/1985 (the year in which the PLD was approved) to the day of the research (17/03/2022) and to limit the search to the Court of Justice. I further refined my research on 02/08/2022 and discovered that the preliminary reference made by Finland was actually handled by the Court[715]. Finally, I checked the CJEU website on 31/01/2023[716] and found out that the last request for a preliminary ruling from France had been addressed, hence I decided, for consistency sake, to find the last judgment on the EUR-LEX database[717]. Consequently, the number of proper judgments increased. I further refined my research by looking for the terms "product liability" AND "Directive 85/374" and selecting English as the main language of the output. The results were 78 entries comprehensive of:

- OJ publications of preliminary references,
- Advocates General's (AGs) opinions,
- judgments of the Court of Justice. In this last category, there were judgments based on Article 267 TFEU (and previous numbers) on the validity and the interpretation of EU law, but not only. There was also a consistent subgroup of judgments based on the actual Articles 258 and 260 TFEU. This means that the judgment was at the end of an infringement procedure due to a "failure to fulfil obligations", used by the Commission to force a MS to make its transposed version of EU law compliant with either the Treaties or the scope of the directive. I noticed that, at the moment, there is still one reference for preliminary rulings concerning the core definitions of the PLD. Hopefully in one year at least the AG opinion will be available.

As a selection method I discarded judgments that mentioned product liability but that were not close to the legislative acts that I have considered in chapter III and with which the PLD has a connection, such as the MDD or MDR. Vice versa, I included other cases because of their relationship to technology as a product. I also included judgments that did not apply the PLD directly, but indirectly through the application of the rules of EU Private International Law.

Following the table, there will be some graphs, to help visualise and quantify the results, which will subsequently be explained. For the latter, I used Excel visualisation tools.

[714] EUR-LEX is the public database of the EU law.
[715] The case is the following "Keskinäinen Vakuutusyhtiö Fennia v Koninklijke Philips N.V., Case C-264/21," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62021CJ0264&qid=1659530426486. Hereinafter *Fennia v Philips.*
[716] See The Court of Justice of the European Union Website, Accessed 31 Hanuary 2022, https://curia.europa.eu/jcms/jcms/j_6/en/.
[717] The case is the following "Cafpi SA and Aviva assurances SA v Enedis SA,Case C-691/21," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62021CJ0691. Hereinfter *Cafpi Aviva v Enedis.*

Case Identifier And Common Denomination	Countries interested	PLD norms concerned	AG Opinion (principles)	CJEU judgment (principles)
C-300/95 Commission of the European Communities v United Kingdom of Great Britain and Northern Ireland Procedure: Article 258 +260 TFEU Facts: In this judgment, the Commission accused the UK of having transposed the PLD in a way that was too tilted towards the producers. All this because of the wording of the English transposition of exception 7(e) concerning the risk development exception	The UK	7(e) risk development exception + failure to fulfil obligations (transposition of said Article deemed to introduce an overly subjective test, while the Commission argued for the objectivity of the criteria contained in Article 7(e) of the Directive	Tesauro §§15-19 description of product liability history in the EU and US and of the rationales of the PLD §20 "[About 7(e)] concept of scientific and technical knowledge at the time when the producer placed the product in circulation is not specifically directed at safety standards in the industrial sector […] but unreservedly, at the state of scientific and technical knowledge, including the most advanced level of such knowledge at the time when the product in question was put into circulation" §§21 "The progress of scientific culture does not develop linearly." Some studies might be disregarded at first but then acclaimed in the scientific community.[…] the state of scientific knowledge cannot be identified with the views expressed by the majority of the learned opinion but with the most advanced level of research that has been carried-out at a given time". §§ 23-25 "one other crucial element is the availability of the information" (comparison with publishing on a US journal and in Manchuria at that time) § 28 AG does not consider that the reference to the ability of the producer made by English CPA, "despite its general nature may or may or even must (necessarily authorise interpretations contrary to the *rationale* and aims of the Directive"	§26 cites opinion AG §20 §27 "[…] the clause providing for the defence in question does not contemplate the state of knowledge of which the producer in question actually or subjectively could have been appraised, but an objective state of scientific and technical knowledge of which the producer is presumed to have been informed" §28 "this state of knowledge implicitly refers to the time it was put into circulation" But §§ 33-39: "The Commission has failed to prove its allegation that the English Consumer Protection Act introduces a subjective criterion to assess the applicability of the risk development exception"
C-203/99 Henning Veedfald v. Århus AmstKommune Procedure: Preliminary reference Facts: Mr Veedfald had to undergo a kidney transplant in an hospital under the responsibility of the Århus municipality. His brother donated the kidney, but the perfusion liquid used in preparation for the transplant was considered to be a defective product by the	Denmark	-Exemptions from liability 7 (a): meaning of putting into circulation 7(c) the product was not manufactured by the producer -Interpretation of the meaning of damage 9 in general: 9(a) damage caused by death or personal injuries	Ruiz-Jarabo Colomer: §14: "the perfusion liquid which should have enabled the transplant was not put into circulation on the market". §15: "the PLD does not apply to services" §17: "the PLD does not apply in this case" But then the AG examines the questions §23: "Producers cannot exempt themselves from liability if a preparation made for their business or organisation is discovered to be defective by arguing it did not put into circulation"	§14: "the directive does not provide a description of the term 'put into circulation'" §15: "the exceptions of Article 7 must be interpreted strictly" §17: "[…] Article 7(a) a product is put into circulation when it is used during the provision of a specific medical service, consisting in preparing a human organ for transplantation and the damage caused to the organ results from the preparatory treatment" §21: the fact that the medical service was done in a public hospital does not make this activity a charitable one as it is paid with tax payers money so exception 7(c) cannot apply. §27: "National legislatures must determine the precise content of the heads of damage (9(a),(b) PLD, save for non-material damage which is regulated solely by national law, full and proper compensation for persons

claimant, Mr Veedfeld. Allegedly the preparation liquid was prepared by the Arhus District Hospital to be used in Skejby hospital where the transplant was scheduled. Mr Veedfeld sued the Århus municipality by claiming he had suffered damages recoverable with the PLD		9(b) damage to, or destruction of any item of property	§26-27: "The fact that the hospital is public does not make it not liable because of a defective preparation because it is free of charge" §§: 28-30: "the damages mentioned in Article 9 should be interpreted according to (now EU) law" § 33: "Damage caused to a human organ which has been removed from the body of the donor for immediate transplantation into the body of the recipient is 'damage caused by personal injuries'; Moreover an organ is not an item of property" § 34: "the laws of each MS have to provide how the victim of the damage must be identified"	injured by a defective product must be available in case of application of those two heads of damage." § 33:" only the national court to examine under which head of damage is at issue. It could also decide not to award any damages if the two heads of damage are not present and despite all the other liability conditions are fulfilled"
C-183/00 María Victoria González Sánchez v. Medicina Asturiana Procedure: preliminary reference A Spanish citizen was infected through a blood transfusion in a clinic called Medecina Asturiana. She sought compensation under national law, whereas the defendant claimed it should have been seeking compensation by relying on the transposition law of the PLD.	Spain	Article 13 PLD: Must it be interpreted that it precludes the restrictions or limitations, as a results of the transposition of the directive, of the rights granted to consumers under the legislation of the MS?	Geelhoed (also for C-52/00) §§35-34: the Directive determines "[…] the full extent of the margin discretion enjoyed by Member States in regulating systems of liability for damage[…] The relevant French and Spanish legislation in these cases must be examined against that yardstick" § 46: "the directive does not contain any reference that suggests a minimum level of harmonization"	§25: "The margin of discretion available to the MS in order to make provisions for product liability is entirely determined by the Directive itself and must be inferred from its wording purpose and structure" §§29-31: the possibility of derogation from the directive "applies only in regard to the matters exhaustively specified and it is narrowly defined" and Article 13 PLD does not provide for such derogation. However, the reference in this article to contractual or non-contractual national liability schemes is not precluded provided those liability schemes are based on other grounds (eg fault or warranty)"
C-52/00 Commission of the European Communities v. French Republic Procedure: 258 +260 TFEU Facts: this is the end of an infringement procedure against France for the incorrect transposition of the PLD.	France	Incorrect transpositions of Articles PLD 3(3) the supplier is equated to the producer whereas it has only an ancillary basis 7 d) and e) PLD 9(b) PLD specifically extension to public property and elimination of 500 EUR threshold 13 PLD Concerning the minimum or maximum harmonization	Geelhoed (joined with medecina) §§ 65-72: "the threshold does not amount to a denial of justice. It was motivated by the need to flood the courts with minor damage to property cases." §§76-79: "The EC had competence not only to regulate liability for defective products but also the procedures related to that (Article 3-3)" §86: "among the conditions to be exempt from liability the French government had added another one which was not in the directive"	§§22-25: "Article 153(now 169 consumer protection) cannot be used retroactively to interpret the directive... The margin of discretion is interpreted according to the directive." Same reasoning than in Medecina Asturiana §28-30: legality of the monetary threshold. Reference to §§66-68 AG's opinion. The Directive is the result of a "complex balancing of different interests" and competition must not be distorted. Moreover, it was done [..] in order to avoid an excessive number of disputes" . 500 euros is not an impossible threshold" see Commission v. Greece § 38: "France is not justified to allege its customary national procedural rule to avoid fulfilment of its EU obligations" §47: while Article 15 of the directive allows the choice of not opting in for the risk development exception "it does not allow [MS] to alter the conditions under which the exemption applied.
C-154/00 Commission of the European Communities v. Hellenic Republic Procedure 258 +260 TFEU	Greece	Incorrect transposition of articles 9 b) PLD 13 PLD	Geelhoed §3: "[…] the subject matter of this case is almost the same as that of Case C-52/00 *Commission v. France* and Case C-183/00 *González Sánchez v. Medecina*	§10: "In that connection, it should be pointed out that the Directive was adopted by the Council by unanimity under Article 100 of the EEC Treaty…concerning approximation of such laws…Unlike Article 100a of the EC Treaty (after amendment, now Article 95 EC), which was inserted into the Treaty after the adoption of the directive and allows for certain derogations, that legal

			Asturiana. As in the present case, the key question in those cases was whether the Directive provides for exhaustive harmonization or whether it involves harmonization at a minimum level". Same arguments as in the two previous judgments §7: "The reference to the national system of private law fails in this case for the reasons set out at paragraph 69 of my Opinion of 18 September 2001" §8: "… Similarly, the fact that a lower threshold of EUR 500 constitutes a reduction in the legal protection already afforded to the consumer by the Greek legislation does not provide any grounds for not transposing in full what is laid down in Article 9(b)"	basis provided no possibility for the Member States to maintain or establish provisions departing from Community harmonising measures" §11: "Nor can Article 153 [consumer protection], likewise inserted into the Treaty after the adoption of the Directive, be relied on in order to justify interpreting the Directive as seeking minimum harmonization of the laws of the Member States which could preclude one of them from retaining or adopting protective measures stricter than the Community measures" §16 "Although Articles 15(1)(a) and 8B) and 16 of the Directive permit the Member States to depart from the rules laid down therein, the possibility of derogation applies only in regard to the matters exhaustively specified and it is narrowly defined […]" §17: "In those circumstances Article 13 of the Directive Cannot be interpreted as giving the Member States the possibility of maintaining a general system of product liability different from that provided in the Directive" §18: "The reference in Article 13 of the Directive to the rights which an injured person may rely on under the rules of the law of contractual or non-contractual liability must be interpreted as meaning that the system of the rules in place… does not preclude the application of other systems of contractual or non-contractual liability based on other grounds, such as fault or a warranty in respect of latent defects" §19: whenever a person wants to rely on a special liability system which existed at the time of notification of the Directive, they must prove that it must be referred to a specific scheme limited to a given sector of production
C-402/03 Skov Æg v. Bilka Lavprisverehus A/S and Bilka Lavprisvarheus A/S v. Jette Mikkelsen and Michael Due Nielsen Facts: two people ate a box of eggs that was infected with salmonella bacteria and subsequently felt sick. They sued the supplier/intermediary (Bilka supermarket) of the defective product and not the producer because of the Danish implementation of the PLD, which in any case joined the proceedings at a later stage.	Denmark	Liability for the supplier of a defective product 3(3) PLD 13 PLD	Geelhoed (Similar reasoning to France Greece and Maria Sanchez) §§46-53: the AG makes a comparison between the French and the Danish PLD implementing provisions of Article 3(3) PLD and finds them structurally similar and with the same end result: they both "extend the class of liable persons to suppliers and other intermediaries in a way which is much more extensive than that provided for in Article 3(3) of the Directive (§51)". It follows from *Commission v. France* that that factor alone [the definition of a wider class of potentially liable people] is sufficient to establish that those rules are not in conformity with the Directive. Moreover, application of the Danish legislation almost inevitably involves an accumulation of proceedings, a result the Community legislature specifically intended to avoid (§53)" §§67-75: In these paragraphs the AG demonstrates that the Danish government's reliance on the 16th statement of the Council as a way to interpret the Directive application. In this statement, the Council expressed the wishes that	§28: "While acknowledging that the possibility of holding the supplier of a defective product liable in accordance with the provisions of the Directive would make it simpler for an injured person to bring proceedings, there would- it was observed- be a high price to pay for that simplicity, inasmuch as, by obliging all suppliers to insure against such liability, it would result in products becoming significantly more expensive. Moreover, it would lead to a multiplicity of actions, with the supplier seeking recourse in turn against his own supplier, back up the chain as far as the producer. Since, in the great majority of cases, the supplier does no more than sell the product in the state in which he bought it and only the producer is able to influence its quality, it was thought appropriate to concentrate liability for defective products on the producer." §34: "Article 3(3) of the Directive provides for the supplier to be liable only in the case where the producer cannot be identified. By laying down in Paragraph 10 of Law No 371that the supplier is to be answerable directly to injured persons, liable against whom the injured person is entitled to bring proceedings under the system of liability laid down by the Directive beyond the limits fixed by the Directive." §39: by citing *Commission v. France*, *Commission v. Greece* and *Gonzalez Sanchez* cases, the CJEU states again that Article 13 PLD could not be used to justify the existence of a national system of product liability which was different from the PLD

			the Member States that were applying rules that were more favourable to consumer protection should keep on applying those rules and not the directive ones in order not to lower the level of protection. AG Geelhoed states that even if that declaration is used to interpret Article 13 PLD, the end result would still be the interpretation he had given previously in other cases, as the PLD "does not preclude maintaining or even adopting, rules on the liability of suppliers provided that such rules relate to fault-based liability and contractual liability (§73)"	
C-177/04 Commission of European Communities v French Republic Procedure 258+260 TFEU Facts: this infringement proceeding is a follow-up of judgment Commission v. France, C-52/00. In this proceeding, the Commission sanctions France which did not change *de facto* its implementing rules on the identity of the producer (it still included the supplier as a first contact subject that could be liable)	France	Failure to fulfil obligations France had not corrected its transposition of Article 3(3) PLD and equated several different actors to the producers	Geelhoed §§52-55: comparison of Article 3(3) PLD and the new French law implementing Article 1386-7 of the French Civil Code. "Comparing the two texts, it is clear, straight away, that the French legislature neglected to include 'the supplier's supplier' in the new wording of Article 1386-7 of the Civil Code. As a result, the transposition of Article 3(3) of the Directive into French law is not yet complete (§55)". The rest of the opinion does not reflect upon the implementation of Article 3(3) PLD but on the procedural fairness of the infringement procedure against France and the calculation of the daily fine.	§22: "In the present case, it is common ground that, on the date of the expiry of the period prescribed in the reasoned opinion of 11 July 2003, the French Republic had not yet taken any measures necessary to comply with the judgment in Case C-52/00 *Commission v France*". §§47-56: The amended form of Article 1386-7 of former French Civil Code transposing Article 3 PLD still did not fully comply with the judgment Case C-52/00 *Commission v France*. Article 3(3) "provides in particular that the supplier cannot incur liability imputed by the Directive 85/374 to the producer where he informs the injured person within a reasonable time of the identity of his own supplier (§50)". "In the present case, it is common ground that such an exclusion of liability does not follow from the wording of the new version of Article 1386-7 of the Civil Code. Consequently, such provision does not fully transpose Article 3(3) of Directive 85/374(§51)"
C-127/04 Declan O'Byrne v. Sanofi Pasteur MSD Ltd and Sanofi Pasteur SA Preliminary reference procedure Facts: A young child got vaccinated against haemophilia and, soon after that, he became mentally disabled. He sued Sanofi Pasteur MSD which was the main distributor of the vaccine in the UK, but it turned out that the producer had been Sanofy Pasteur SA, in France. In this context he risked being time-barred to bring the action against the real producer as the producers' liability lasts only ten years and the proceedings against the fake producer had lasted for a long time before coming to the conclusion that Sanofi Pasteur was the actual defendant.	The UK	Placing in circulation in the context of the exemption in Article 7 a) PLD when there is a supply of defective product by producer to a wholly owned subsidiary 11PLD time barring or bringing the action against the producer	Geelhoed §§ 22-28: recalls the Veedfald judgment as it is similar but "this case focuses on when to calculate when a product has been put into circulation and not whether the product had been put into circulation" §§38-40: "there is not an agreement on when to apply the putting into circulation moment for intragroup transactions as in the present case" §§31-51: very elaborate analysis on the diversity of organisation in multinational companies. "[…] It would be unfair to consider the moment of putting into circulation the delivery of the product from a branch to another affiliate company of the same group… Therefore, putting into circulation in this case coincides with the moment in which the product exits the sphere of control of the group." §65: "[…] it is not contrary to the Directive, in particular to Articles 3(3) and 11, to permit the court to	§30: It is left to the national courts to decide, having regard to the specificities of the case, "[…] whether the links between the producer and another entity are so close that the concept of producer within the meaning of Articles 7 and 11 of the directive also include the latter entity and that the transfer of the product from another of those entities does not amount to putting into circulation within the meaning of the provisions." §35: "The class of people/subjects described in Articles 1 and 3 of the directive that can considered to be liable must be considered exhaustive" (reference to Skov Æg) §38: When a national court decides the rules governing "[….] the substitution of one party to another must ensure that due regard is had to the personal scope of the directive, as established by Article 3 thereof."

			lodge a claim brought by a plaintiff against the producer when the supplier knew who the producer was and could have informed the plaintiff."	
C-327/05 Commission of the European Communities v Kingdom of Denmark Procedure: 258 + 260 TFEU	Denmark	Failure to fulfil obligations Liability of a supplier for a defective product Article 3(3)	Not available	§1-2: The Court finds that despite the Skov Æg judgment, "Denmark had not complied in changing the Article of the law transposing Article 3(3) of the PLD"
C-285/08 Société Moteurs Leroy Somer v Société Dalkia France, Société Ace Europe Facts Societé Dalkia France and its insurer had sued Société Moteurs Leroy SA because the generator it had provided was defective and caught fire in a company. According to French law, the defendants could ask for damages from the producer even if the generator was used for professional activities. Société Moteur Leroy argued that it could not be sued under the PLD	France	Damage to an item of property intended for professional use Article 9 b)i) PLD 13 PLD	Mengozzi Not available	§§22-24: Reference to Skov Æg. "The system of the directive precludes the national system rules only if the national system is covered by the scope of application of the directive" §25: "from 18th recital of the PLD it is apparent that the PLD does not seek to exhaustively harmonise the field of liability beyond the matters it expressly regulates." §27: "Article 9 by defining damage does not extend to professional activity." §31 As a consequence, harmonization of the PLD does not extend compensation for damage to an item of property intended for professional use. Hence the "[…] directive does not prevent a Member state from providing in that respect for a system of liability corresponding to that established by the directive"
C-358/08 Aventis Pasteur SA v. OB Procedure: reference for a preliminary Ruling Facts: OB received a haemophilius vaccine in 1992. It was distributed by MériauxUK Ltd, an English company, that was owned entirely by Pasteur Méreux Sérums et Vaccins SA, which later changed its name to APSA. OB reported severe brain injuries after the injection and was convinced the vaccine was the cause of his brain injuries despite doctors finding the cause in the herpes simplex virus infection. APSA in the meantime formed a joint venture with Merck Inc. of the US. Mériaux UK became the United Kingdom subsidiary. It became Aventis Pasteur MSD (APMSD). OB brought an action against APMSD before the High Court of Justice. APMSD contended it was just the distributor, not the manufacturer. OB brought action against APSA but OB was actually time-barred.	The UK	Articles 3(3) PLD 11 PLD very similar facts to the judgment O'Byrne v Sanofi	AG Trstenjak §§34-39: in O'Byrne the CJEU opted for a functional interpretation of the concept of producer. In order to describe this functional approach, the AG outlies the multi-layered concept of producer. In O'Byrne, it regarded the whole distribution chain may be regarded as the producer as in Article 3(1) PLD because of its involvement in the manufacturing of the product. "National courts have to determine whether a supplier is to be classified functionally as producer. In particular whether the producer retains de facto control over the product transferred." §75: "consumer protection, competition and movement of goods are all objectives of the directive and none of them prevails over the other two" §80: "the procedural rule for substitution of parties in order to have a producer even if the 10 year liability have expired is against the directive"	Inverse order of dealing with questions. First there is the issue of Article 11 which takes the view of AG but also adds the importance of the legal certainty principle (§§37- 49) As far as the definition of Producer § 56 the supplier must be treated as producer "if he has not informed the injured person, within a reasonable time, of the identity of the producer or his own supplier."

C-495/10 Centre hospitalier universitaire de Besançon v Thomas Dutreux and Caisse Primaire d'assurance maladie du Jura Procedure: reference for a preliminary ruling. Facts: A 13 year old boy suffered severe burns because of a defective warmed up hospital bed mattress. The hospital claimed that only the producer of the defective mattress had to be held liable	France	Article 13 And whether the PLD limits liability national system	Mengozzi §§27-32: differences in the directive between producer and supplier citing previous case law and making differences with Directive 2001/95. The conclusion is that "CHU Besançon cannot be considered distributor of the defective mattress and cannot be equated with supplier" §§45-46: the coexistence of the two systems (PLD and national fault based system for service provider)	§§26-27: "The PLD does not regulate the supplier's liability. Liability may be incurred if the product is not among the matters regulated so it does not fall within the scope of the directive"
C-496/12 Request for preliminary ruling	Slovakia	Whether Dir 85/374 must be applied to juridical people. Removed	NA	NA
C-45/13 Andreas Kainz v. Panterwerke AG Facts: An Austrian cyclist was injured in Austria with a bike that was purchased from a German seller. He argued that the jurisdiction should be in Austria and not in Germany (EU private international law with special reference to consumer protection and PLD)	Austria	Liability for defective product + Regulation 44/2001	Not available	§31: "Article 5(3) of Regulation No 44/2001 is specifically not designed to offer the weaker party stronger protection (see, to that effect, Case C-133/11 Folien Fischer and Fofitec [2012] ECR, paragraph 46), but it should also be noted that the interpretation proposed by Mr Kainz that the place of the event giving rise to the damage is the place where the product in question was transferred to the end consumer or to the reseller likewise does not guarantee that that consumer will, in all circumstances, be able to bring an action before the courts in the place where he is domiciled since that place may be elsewhere or even in another country.
C-310/13 Novo Nordisk Pharma GmbH v S. Reference for a Preliminary ruling Facts: From 2004 to 2006, Ms S. received injections of Levemir, a medicine produced by Novo Nordisk Pharma. This caused her to suffer lipoatrophy. Ms- S asked the Landgericht Berlin to order Novo Nordisk Pharma to disclose information on side effects of Levemir in connection with lipoatrophy by relying on Article 84a of the special medicinal law in Germany (AMG). The Landgeright agreed as well as the Kammergeright in Berlin. Novo Nordisk Pharma brought the proceedings to the Bundesgerightshof, which made the reference to the CJEU. The court wants to understand whether the outcome of the appeal relates to the right of information in §84a of the AMG and depends on whether such provision infringes the PLD.	Germany	Special liability system AMG is compatible wihArt.13PLD And 4PLD concerning proof	Szpunar §26: Interpretation of the Article 13 PLD in relation to other kinds of liability (contractual- non contractual liability). Doubts arise concerning the "moment when this directive is notified" as the German law for pharmaceutical products was existing before the PLD §30: "the time frame indicated by Article 13 PLD relates to the special liability system and not to contractual or non-contractual system. For no-fault liability rules, they remain unaffected as long as they pre-date the directive. However, this would make the PLD meaningless." §31: In any case the derogation in Article 13 PLD concerns "not the liability system but the rights of injured persons" §34: "The German AMG system falls within Article 13: it is limited to a specific production section and did not have a general nature like Spanish law in Maria Sanchez. Hence the AMG is admissible." §36: "Despite the rule in Germany where adverse effects of medicinal products are excluded by the PLD but they are not excluded from the harmonization by PLD"	§ 20: "As a preliminary point, it should be noted that, under Article 13 of Directive 85/374 that directive does not affect any rights which an injured person may have under a special liability system existing in the date the directive was notified" §21" As the Advocate General noted in point 34 of his Opinion, the German system of liability for pharmaceutical products, established under the AMG, constitutes such a special liability system for the purposes of Article 13 of Directive 85/375 in so far it is limited to a specific manufacturing sector and it existed on 30 July 1985, the date in which the directive was notified to the Federal Republic of Germany". §25 "As regards the consumer's right to obtain information on the adverse effects of a product, it should be noted that neither that right nor the scope of the information that the consumer could require the manufacturer if that product to provide are covered, as such, by directive 85/374" §26-29: "The fact that the AMG makes it possible for the plaintiff to ask for information on the product makes it easier for them to prove the liability of the manufacturer, but this is "not among the matters governed by Directive 85/374 and that, accordingly, it falls outside the scope of the directive (§29)". §31: "National legislation such as that at issue… does not compromise the effectiveness of the system provided for under Directive 85/374 or the objectives pursued by the directive"

			§43: "Article 13 allows as part of a special liability system the rights of injured persons going beyond the level of protection conferred by the directive to be preserved only if those rights were already in existence before the directive was notified" §47: "the right to obtain information on adverse medical effects is covered by Article 4"	§32: "…such national legislation is only intended to eliminate the significant imbalance which exists between the manufacturer of the relevant product and the consumer…"
C-503/13, C-504/13 Boston Scientific Medezintechnik GmbH v AOK Sachsen-Anhalt(503) v Betriebskrankenkasse RWE (504) Procedure: Reference for a Preliminary ruling 267 TFEU Facts: The facts consisted in the discovery of a potential malfunctioning in pacemakers and defibrillators. Whether a potential defect of a product had to be considered as an actual one was the main question	Germany	Article 1 Article 6(1) defectiveness Article 9a) damage and personal injury	Bot §29: "[…] the concept of defect is to be assessed in the abstract with reference not to a specific user, but to the public at large, having regard to a standard of safety that the consumer might reasonably expect. The objectivity of the concept of defect is tempered, however, by the fact that more specific circumstances are taken into account 'including' the use" §30: concept of "safety which a person is entitled to expect is relatively imprecise…Interpreted in the light of the objective, set-out in the second recital… that concept must be understood to refer to a product that poses risks jeopardising the safety of its user and having an abnormal unreasonable character exceeding the normal risks inherent to its use". §31: "… In the light of that definition, I take the view that the mere possibility of failure in the pacemakers implanted in B and in W and the defibrillator implanted in F constitutes a defect for the purposes of that article, since it is reasonable to expect there to be such a safety failure, irrespective of whether it has been specifically established that those products actually had the inherent fault identified by the manufacturer". §36 "… That conclusion is not affected by the fact that the legal basis of Directive 85/374 is Article 100 of the EEC Treaty, which became Article 94 EC, then Article 115 TFEU, concerning the approximation of such laws, regulations and administrative provisions of the Member States as directly affect the establishment or functioning of the common market. Even though that provision offers no possibility for Member States to maintain or establish provisions departing from Community harmonising measures, (12) including the provision of a higher level of consumer protection, this does not mean that harmonising measures adopted on its basis do	§40 quote §30 AG §55 opinion of AG is accepted also concerning damages but needs to be assessed by national courts

			not have the objective of guaranteeing consumer protection." §38: "…Making proof of a lack of safety subject to the actual occurrence of damage would disregard the preventive function assigned to EU legislation on the safety of products offered on the market and to the specific liability regime established by Directive 85/374, (13) which manifestly pursues a preventive function by imputing liability to the person who, having created the risk most directly by manufacturing a defective product, is in the best position to minimise it and to prevent damage at the lowest cost" §41:In so far as human health protection requirements must be integrated into all Union policies, such protection must be regarded as an objective that also forms part of the policy calling for the harmonization of the Member States' rules on liability for damage caused by defective products. §42: In the light of that objective, the function of health products for human use lends such products an indisputable specific character, which must be taken into account in assessing the concept of defect. §64:"… Moreover, the Court has already ruled, in *Veedfald*, (25) that although Article 9 of Directive 85/374 neither contains any express definition of the term damage nor determines the precise content of the heads of reparable damage, it must be interpreted as requiring full and proper compensation for persons injured for the heads of damage covered by the term, save for non-material damage whose reparation is governed solely by national law" §66: Accordingly, all material loss or damage resulting from personal injury must be compensated for in full. §73: "… Lastly, is there any need to state that the present cases are taking place against the specific background of an increase in the number of health scandals involving health products, in particular implantable medical devices such as artificial hip joints, cardiac leads, knee joints or breast implants?... As these scandals have highlighted the gaps and weaknesses in the present authorisation and control system […]"	

			§74: AG recognises "compensation may be awarded in respect of damage caused by action intended to avert a risk of much more serious damage is likely to prompt producers to improve the safety of their products" §75: "even the preventive surgical operation to remove the defective device constitutes damage for personal injuries"	
C-219/15 Elisabeth Schmitt v TÜV Rheinland LGA products GmbH Facts: Ms Schmitt had undergone a breast reconstruction intervention and the prostheses used were manufactured by PIP. After the surgery it was discovered that PIP manufactured those prostheses with industrial silicone gel and not the specific one for this kind of prostheses. Because of the fraud, PIP went bankrupt. Ms. Schmitt decided to undergo more surgery to explant the defective prostheses and have new implants. Because PIP had filed for bankruptcy she brought action against TÜV, the notified body (NB), that should have certified the conformity of the prostheses, according to the Medical Devices Directive (Directive EC 93/42). TÜV claimed that the directive did not establish any kind of liability between an NB and a patient, as there was no contractual relationship between them.	Germany	Not the PLD directly but MDR (producer had gone bankrupt see interest chapter II and III, in particular choice of more protective liability regime)	Sharpston §24: The birth of the New Approach (see chapter III) is the *Cassis de Dijon* case because MS cannot forbid or restrict the marketing of products on the basis only of non-conformity requirements. "[…]the Court opened the door to a reflection on how goods could best be marketed in the European Community" §26: The MDD "[…]must reconcile the free movement of medical devices with the protection of patient's health" §33: "[…] it is clear that [Directive 93/42] imposes primary responsibility for compliance of the product on the manufacturer" §34: "Plainly, however, that directive does not limit the obligations as to product safety on the manufacturer alone" as it also imposes duties on Member States." §35: "The directive is silent as regards the imposition of liability on notified bodies, although the requirement under section 6 of Annex XI that they take out civil liability insurance makes it clear that liability for something is contemplated. May the notified bodies be liable to users of those devices in the event of a culpable failure on their part to fulfil their duties?" §39: "Given their crucial role played by notified bodies in the procedure leading to the placing on the market of medical devices… it seems to me entirely appropriate that those bodies should in principle be capable of bearing responsibility under national law… provided always that the principles of equivalence and effectiveness are respected. That will be a matter for the national court to determine" § 42: The duties imposed on notified bodies could be "[…]either general in nature, that is to say,	§40: "[…] the provisions of Annex II to Directive 93/42 do not impose a general obligation on the notified body to carry out unannounced inspections, to examine devices and/or to examine the manufacturer's business records." §42: "[…] It is apparent from Section 5.4 of the annex [Annex II] that the notified body may pay unannounced visits to the manufacturer during which it may, where necessary, carry out or ask for tests in order to check that the quality system is working properly." §51: "[…] the manufacturer is responsible for the security of the device in the first place, but the MDD also imposes obligations on Member States and Notified bodies " §55 : "It should be noted at the outset that the Court has previously stated that it does not necessarily follow from the fact that a directive imposes surveillance obligations on certain bodies or the fact that one of the objectives of the directive is to protect injured parties that the directive seeks to confer rights on such parties in the event that those bodies fail to fulfil their obligations , and that is the case especially if the directive does not contain any express rule granting such rights". §56: "[…] in the absence of any mention in Directive 93/42 of the manner in which civil liability of notified bodies may be incurred, it cannot be maintained that the purpose of the directive is to govern the conditions under which the end users of medical devices may be able to obtain compensation for culpable failure by those bodies to fulfil their obligations" §58: "It is established case law that the system of rules put in place by Council Directive 85/374/EEC …on the approximation of the laws, regulations and administrative provisions of the Member States Concerning liability for defective products … does not preclude the application of other systems of contractual or non-contractual liability based on other grounds such as fault" (see Skov Æg) §59: "It is national law that establishes the conditions because of which a Notified Body can be considered liable, provided that the principles of equivalence and effectiveness"

			there is an obligation to perform them on a regular basis and without due cause of any kind; or they may be particular, that is to say, that the notified body is required to undertake them only where there is a reason for it to do so". §45: "[…]the role of notified bodies is primarily a scientific one… They are not law enforcement bodies" §54: "[…] However, it seems to me that, as part of a general duty of diligence, a notified body is under a duty to be alert …If, therefore, it is put on notice, whether as a result of information arising out of its own inspections and assessments or otherwise, it will be under a duty to act.	
C-621/15 N.W. and Others v. Sanofi Pasteur MSD SNC and Others Reference for preliminary ruling 267 Facts Mr W. was given a vaccine against hepatitis b through three injections. Soon after his health worsened until he reached the diagnosis of multiple sclerosis, which in one year-long time brought him to a 90% level of invalidity. His relatives and himself were convinced of the connection between the vaccine and the appearance of the first symptoms of the illness, as there was no familiarity with multiple sclerosis in Mr. W. family. Mr W and his relatives sued Sanofi Pasteur and claimed that the Cour de Cassation doctrine actually allowed the use of presumptions whenever they were serious, specific and consistent. However this argument was not accepted in the appeals phase. After the Court of Cassation reversed the appeals judgment, another Court of Appeals (Paris) observed that those presumptions were not supported by any specific scientific claims, therefore it reversed the judgment. Mr W and his family went again to the Cassation phase and the Court made a reference to the CJEU asking how legal presumptions needed to be evaluated in the context of the PLD (the regime which applied to the vaccines in France)	France	Article 4 PLD: causal link and proof of defect and damages suffered for vaccinations hepatitis B;	Bobek §16: "the standard of proofs to demonstrate the damage and the causal link are not harmonised by the PLD. In theory it is matter of national law, but EU imposes certain limits to the proof of evidence" §24: if MS lay out the rules on proof of evidence it must respect the EU principles of equivalence and effectiveness §28: the meaning of 'legal presumption' may vary in the MS but in French is "a method of legal reasoning" based on inference. §34 :Bobek establishes an harmonised concept of presumption as circumstantial evidence or indirect proof §39 Article 4 does not preclude factual presumption which the judge is free to use §42-44 the directive does not require the proof of scientific causation §45 there would be a risk of conflict with the principle of effectiveness if the national rules on proof i)explicitly prohibit judges from taking potentially relevant evidence into account or identify specific pieces of evidence as systematically constituting conclusive and non-rebuttable evidence of a given fact 77-100: rules on causation and defect also follow the ones on presumption. Meaning that they must not harm the effectiveness of EU law	§21: "From the 18th recital it is clear that the PLD does not want to exhaustively harmonise the sphere of liability for defective products beyond the matters regulated by it (§24 *Novo Nordisk Pharma*)" §22: "The PLD does not contain any reference to the significance of causal relationship, contrary to the concept of defect." §24: "The PLD does not regulate aspects relating to the proof of damage" §25: " … under the principle of procedural autonomy and subject to the principles of equivalency and effectiveness it is for the national legal order of each Member State to establish the ways in which evidence is to be elicited.." §26: " Regarding more specifically the principle of effectiveness, it requires, in terms of the detailed procedural rules governing actions for safeguarding rights which individuals derive directly from EU law, that those rules do not render practically impossible or excessively difficult the exercise of the rights conferred by EU law" §33: "the French national evidentiary rules are neutral as to the burden of proof of Article 4 and "…are in principle capable of preserving the effectiveness of the system of liability provided for" by the PLD. Despite all this the actual scope of such rules must be determined in the light of the interpretation and application given to them by national courts" §§34-36:" It can happen that courts apply those rules in an 'overly rigorous manner' (AG opinion 54, 60 and 75) or the contrary, with the danger of creating an immediate and automatic presumption 'where one or more types of factual evidence were presented together'" §37: " Therefore, the national courts must first ensure that the evidence adduced is sufficiently serious, specific and consistent to warrant the conclusion that, notwithstanding the evidence produced and the arguments put forward by the producer, a defect in the product appears to be the most plausible explanation for the damage, with the result that the defect and the defect and the causal link may reasonably be established"

C-581/18 RB v TÜV Rheinland LGA products GmbH and Allianz IARD S.A. Facts: The plaintiff is a German national who, in autumn 2006, underwent breast surgery in Germany with prostheses made in France by PIP and marketed in the Netherlands. In March 2010 it was discovered that the French prostheses were defective, and PIP went bankrupt. The German authorities recommended doctors to alert the patients and un 2012 they recommended to remove the defective prostheses. The plaintiff brought action against the notified body (see case Schmitt supra) and Allianz IARD who was the insurer of PIP. Allianz IARD however put a territorial delimitation clause: it would pay the damages only to people on the French territory. According to the plaintiff this was a violation of the principle of non-discrimination, Article 18 TFEU	Germany	Not the PLD directly but the application of the principle of non-discrimination (article 18 TFEU) by the insurer of the bankrupt company (the producer had gone bankrupt see interest chapter II and III, in particular choice of more protective liability regime, here in the specific the possibility to apply the best insurance policy	Bobek §22: "..can Article 18 TFEU be directly relied on horizontally by the appellant against Allianz or vertically (or, rather, diagonally) against the French Republic(?)" §23: "All the questions share an unspoken assumption, namely that the territorial limitation at issue is not only within the scope of EU law, but also discriminatory on grounds of nationality and contrary to Article 18 TFEU" §24: it is necessary to understand whether the issue is within the scope of EU law and which provision of EU law could lead to find the territorial limitation unlawful §28: The case is within EU law as "for the jurisdiction of the Court to be triggered, there needs to be a sufficiently clear and direct link between the case at hand and one of the fundamental freedoms (free movement of goods, persons, services or capitals) (1) and /there must be a potentially applicable provision (secondary) EU law in need of interpretation for the case at hand (2) §30: the case law on the provisions on the fundamental freedoms expanded also to situation in which people were dissuaded by exercising their freedom and when the mere cross-border potentiality is sufficient. The limits to this potentiality are established with *Keck* judgment for goods but not for the remaining economic freedoms. §37: "In the absence of any actual or potential cross-border element, a connecting factor sufficient to trigger EU law is the existence of relevant, potentially applicable legal rules laid down in (secondary) EU law that do not make any distinction between activities having a foreign aspect and acrivities that have no such aspect. Thus, unless the scope of the measure is expressly limited to situations having a cross-border dimension, the existence of harmonising measures and the need to interpret them in relation to the case at hand may constitute a sufficient link to trigger the application of the EU" 41§: This case is within the scope of the EU because of the "1) cross-border element in the context of the free movement of goods and its consequence in terms of liability 2) the potentiality with regard to freedom to receive (insurance)	§56: "…the dispute in the main proceedings relates not to the cross-border movement of goods in itself, but to the harm caused by the goods that have been so moved…" §57:" Consequently, the situation at issue in the main proceedings is not linked by any specific connecting factor to the provisions of the FEU Treaty on the free movement of goods"

			services from another Member State; and (iii) the normative subject matter of the case, namely manufacturers' liability for defective products and medical devices as goods in the internal market" §49: the main problem is that the referring court only refers to Article 18 TFEU without identifying any other rule which has been infringed under discriminatory considerations. §52: Article 18 TFEU is referred to in relation to other provisions §56: can it be connected to the Medical Device Directive? Or regulation? There is not yet an insurance obligation for manufacturers under Article 10(16) §75: why does the mandatory French insurance obligation not travel to Germany? Is it a barrier to free movement? §76: the answer is no because the insurance is not covered by article 34 or 35 TFEU §80 it follows that the Treaty rules on the free movement on goods are not applicable to the conditions concerning the subsequent use of goods in the host Member state §109: if one interprets Article 18 in the sense that in this case there was indirect discrimination, there would be other structural problems: "[…] Article 18 would be turned into a limitless provision, by virtue of which any issue, however remotely connected to a provision of EU law could be harmonised by judicial means. It would furthermore turn regulatory competence within the internal market on its head, generating irreconcilable future conflicts of competence between Member States." §119 : "The fact that the MDD does not say anything about how to transfer an insurance from one country to another means that it is not within the competences of the Court to extend fiscal policy of EU."	
C-65/20 VI v. KRONE- Verlag Gesellschaft mbH &Co KG Copy of a newspaper containing false health advice	Austria	Article 2 PLD	Hogan §§33 "mere information is not a product…" hence the PLD does not apply"	§37: "[…] the fact that no provisions are made in Directive 85/374 for the possibility of defective products in respect of damage caused by a service of which the product is merely the medium, reflects the intentions of the EU legislature." §39: "…inaccurate health advice which is published in a printed newspaper and concerns the use of another physical item falls outside the scope of Directive 85/374

				and is not such as to render the newspaper defective and the 'producer' strictly liable pursuant to that directive, whether they are the publisher or the printer of that newspaper or even the author of the article."
C-410/19 *Software incubator* Post-Brexit case but submitted before it was effective, hence CJEU competence and jurisdiction Facts: *Computer Associates* created a software and entered into agreement with Software Incubator, a company which had to make the software (the product) known in the UK and Ireland. It was an agency contract between the principal (Computer associates) and the agent (Software incubator).. The software was supplied by Computer associates through a link in an email which led to a portal. From this portal the users could download the software. Computer Associates had also the exclusive right to determine the terms and conditions in connection with licensing of the software. The Software incubator function was focused on the promotion of the software and did not have any authority to transfer title or property in the software. The customer was granted a perpetual licence. This licence allowed the customer to download and install the software in a specified territory to a limited number of end-users. Computer associates retained all the IP. In 2013 Computer associate terminated the agreement with Software incubator which brought an action against Computer Associates. The High Court stated that the perpetual licence of software amounted to a sale of goods according to Article 1(2) of Directive 86/653 and awarded 475,000 £ to the Software incubator as compensation for being an agent. Computer Associate lodged an appeal against the judgment before the Court of Appeals. The Court held that the software, not being a tangible medium, could not be considered as goods. The Supreme Court granted the Software incubator permission to appeal which also decided to stay the proceedings.	The UK	Discussion of wording of Directive 86/653 on self-employed commercial agents 1)Where a copy of computer software is supplied to a principal's customers electronically, and not on any tangible medium, does it constitute "goods" within the meaning of that term as it appears in the definition of a commercial agent in Article 1(2) of Council Directive 86/653/EEC of December 1986 on the co-ordination of the laws of Member States relating to self-employed commercial agents ("Directive")? (2) Where computer software is supplied to a principal's customers by way of the granting to the customer of a perpetual licence to use a copy of the computer software, does that constitute a "sale of goods" within the meaning of that term as it appears in the definition of commercial agent in Article 1(2) of the Directive?	Tanchev §22: "Brexit happened during the proceedings, but the Court has jurisdiction for cases submitted before 31 January 2020. Therefore, the CJEU is competent and has jurisdiction on the case" §38: "The Court asks whether computer software can be considered a good in the context of Article 1(2) of Directive 86/653. It is necessary first to clarify the application and significance of the concept of agent in the Directive, the impact of the judgment UsedSoft, and the interpretation of the concept of 'goods' and 'sale'." §44: "The agent is: 1) a self-employed intermediary; 2) connected to another subject by a contractual relationship with a continuing character and 3) deals with negotiating the sale or purchase of goods for the principal or in negotiating and concluding such transactions in the name and on behalf of the principal. These conditions are necessary and sufficient" §47: In the used soft judgment the Court considered that in the context of Directive 2009/24 Article 4(2) on the legal protection of computer programs sale had the following meaning: "an autonomous concept of EU law,[…] an agreement by which a person, in return for a payment, transfers to another person his rights of ownership in an item of tangible or intangible property belonging to him". And it did not make any difference how the computer program was made available to the buyer. §54: "[…] I have come to the conclusion that electronically supplied computer software, such as that at issue, falls within the concept of 'goods' for the purposes of Article 1(2) of Directive 86/653. " §55: "In the directive nobody specifies what a good is."	§30: "In those circumstances, the concept of 'sale of goods' must be given an autonomous and uniform interpretation throughout the European Union, in the light of the need for the uniform application of EU law in conjunction with the principle of equality. That concept therefore constitutes an autonomous concept of EU law and its scope cannot be determined by reference either to concepts known to the laws of the Member States or to classifications made at national level (see, by analogy, judgment of 9 July 2020, RL (Directive combating late payment), C-199/19, EU:C:2020:548, paragraph 27 and the case law cited)" §31: "In that regard, it should be borne in mind that the meaning and scope of terms for which EU law gives no definition must be determined by considering their usual meaning in everyday language, while also taking into account the context in which they occur and the purposes of the rules of which they are part (judgment of 4 June 2020, Trendsetteuse, C-828/18, EU:C:2020:438, paragraph 26 and the case law cited" §32: " It is in the light of those considerations that it must be determined whether the concept of 'sale of goods' in Article 1(2) of Directive 86/653 can cover the supply, in return for payment of a fee, of computer software to a customer by electronic means where that supply is accompanied by the grant of a perpetual licence to use that software."

C-264/21 Keskinäinen Vakuutusyhtiö Fennia v. Koninklijke Philips N.V. Procedure: Preliminary reference 267 TFEU Facts: A coffee machine produced by Philips (Dutch company) and partly manufactured by Saeco, Rumania, a subsidiary of Philips, caused a fire accident in a home in Finland. The insurer, Fennia, after having compensated the consumer under a home insurance policy, requested Philips to pay for damages (EUR 58 879,10), being it the producer of the object and both Philips and Saeco trademarks were owned by Philips. Philips objected that it could not be considered the producer as also Saeco had put its trademark and its name on the object	Finland	Article 3(1) §25 "Must [Article 2 and Article 3(1) of Directive 85/374] be interpreted as meaning that an electricity distribution system operator may be regarded as a "producer" if it alters the voltage of the electricity from the supplier so that it may be distributed to the final consumer?"	Ćapeta Not available	§26: "Thus, Article 3(1) of Directive 85/374 contains, in essence, an alternative, only the first part of which concerns the person who is at least partially involved in the process of manufacturing the product. By contrast, the second part of the alternative refers to a person who presents himself as a producer by putting his name, trade mark or other distinguishing feature on the product." §27: "It is therefore apparent from the clear and unambiguous terms of that provision that the involvement of the person who presents himself as a producer in the process of manufacturing the product is not necessary in order for such person to be classified as a 'producer' within the meaning of that provision." §32: "[…] According to the fourth recital of Directive 85/374, protection of the consumer requires that any persons who present themselves as producers by affixing their name, trade mark or other distinguishing feature to the product should be made liable in the same way as the actual producer. Furthermore, it follows both from Article 5 of that directive and from the fifth recital thereof that the liability of a person who presents himself as a producer is on the same level as that of the actual producer, and that the consumer may freely choose to claim full compensation for damage from any one of them, since they are liable jointly and severally." §33: "It thus appears that the purpose of Article 3(1) of Directive 85/374 is to ease the burden of having to determine the actual producer of the defective product in question. In that regard, it is apparent from the explanatory memorandum relating to Article 2 of the Commission's proposal for a directive of 9 September 1976, which gave rise to Directive 85/374, taking into account that that article became, without substantive amendment, Article 3 of that directive, that the EU legislature considered that the protection of the consumer would be insufficient if the distributor could 'refer' the consumer to the producer, who might not be known to the consumer." §37: "Accordingly, contrary to what Koninklijke Philips maintains, it must be held that, in the case in the main proceedings, a division of liability between that company and Saeco International Group has no effect in relation to consumers, who must specifically be relieved of the burden of having to determine the actual producer in order to bring claims for damages".
C-691/21 Cafpi SA, Aviva Assurances SA v Enedis SA Procedure: Reference for a preliminary ruling. In an agency of the Cafpi company there was a malfunctioning of the electrical equipment due to a voltage surge. Aviva, Cafpi's insurer, compensated Cafpi. Later, Cafpi and Aviva decided to start a legal suit together against Enedis, the electrical energy distributor, as they claimed that it was the	France	2 PLD 3(1) PLD	Not Applicable	§34 "As a preliminary point, in so far as the referring court refers, in its question, to Article 2 of Directive 85/374, it should be observed that that article contains the definition of the term 'product' and, in that context, expressly provides that electricity must be regarded as a product within the meaning of that directive." §35 "The class of liable persons against whom an injured person is entitled to bring an action under the system of liability laid down by Directive 85/374 is defined exhaustively in Articles 1 and 3 of that directive. Since that directive seeks to achieve complete harmonization in the matters regulated by it, its determination in those articles of the class of liable persons must be regarded as exhaustive and cannot be made subject to the setting of additional criteria which do not follow from the wording of those articles."

producer according to the PLD despite it was formally only an electricity operator distributor. Enedis denied being the producer hence the preliminary reference made by the Cour d'appel de Versailles. In the end, the previous *Fennia v Philips* judgment was used to confirm that the electricity operator distributor had to be regarded as the producer				§39: "In the second place, as regards the context of that provision, it must be observed that it is clear from Article 5 of Directive 85/374 read in the light of its fourth recital that, in respect of the same product, several persons may be classified as the 'producer' within the meaning of Article 3(1) of that directive and, on that basis, all those persons are to be jointly and severally liable for the damage caused by that product." §43 " The concept of 'producer', within the meaning of Article 3(1) of Directive 85/374, which is an autonomous concept of EU law, thus meets the objective of consumer protection, which requires, first, that several persons may be regarded as producers and, second, that consumers may bring claims against any one of them, so that the search for a single liable person, that is to say, 'the most appropriate person' against whom consumers should assert their rights, is not relevant".

Table 1

2.1. First quantitative and qualitative analysis of EU PLD-related cases: number and types of cases per Member State.

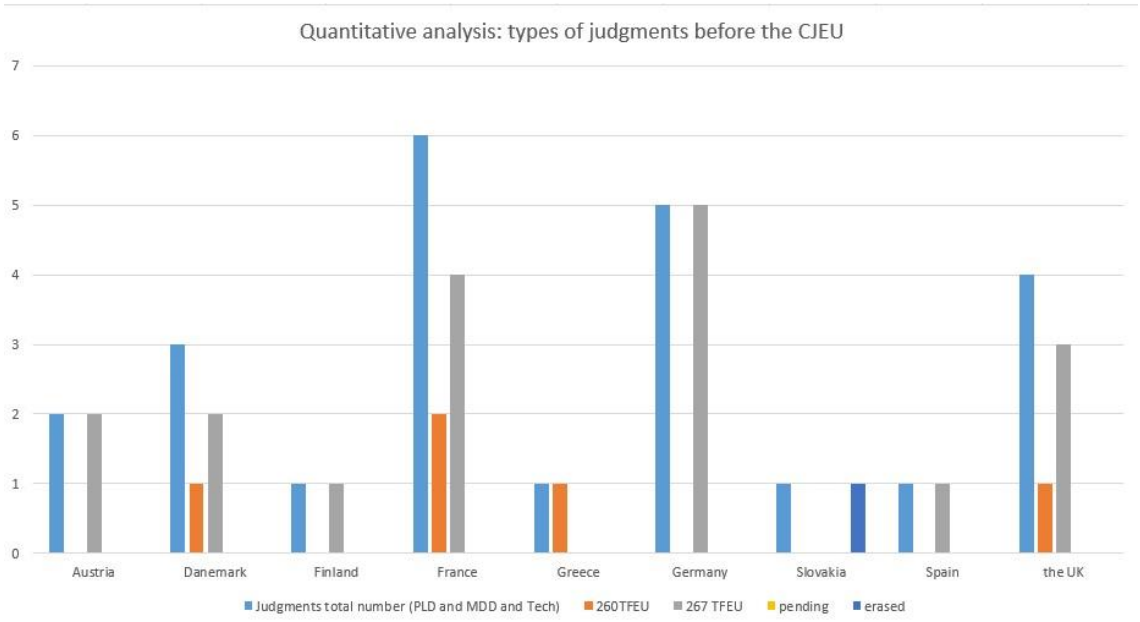

Figure 2

Based on the previous table, I will try to apply both a quantitative and subsequently a qualitative analysis to the above summarised judgments. To achieve these objectives, I will try to find patterns through the help of visualisation

tools provided by Excel software. The first attempt made concerns a quantitative analysis of the judgments which were about the PLD and also the ones citing the PLD as a model from which to take inspiration[718]. Overall, Figure 2 tries to find how many judgments per country there were, and which type of procedure was more frequently used (both per single country and in general).

By analysing the previous judgments selected according to the above-mentioned criteria, the MS that has more judgments in absolute terms concerning the PLD is France which also has the three kinds of judgments selected: 4 preliminary reference procedures, 2 infringement/failure to fulfil obligations proceedings making a total of 6 cases. Among these cases there was almost always the same common themes, which were the application of Article 3 PLD, concerning the identity of the producer[719] and also the application of Article 13 PLD, concerning the relationship with other systems of liability. Other important themes in the French judgments were the application of Article 4 PLD[720] on the causal link and how to prove it, of some of the exceptions of Article 7[721], and the application of Article 9, especially its letter b), i) and ii) concerning the damage to private property[722]. It is interesting to notice that the issue concerning the precise identity of the producer and whether that is connected to the field of application of the PLD is still debated in France as Article 3 PLD was the core of the latest judgment mentioned in Table 1, *Cafpi Aviva v Enedis*[723].

Germany immediately follows France in this "race", with 4 cases in total. Nevertheless, two of the judgments considered are connected to the PLD in an indirect way through Notified Bodies' (NB) liability in the former MDD and its system of safety certification and insurance for medical devices. The PLD is mentioned several times, with reference to the principle that the producer/manufacturer is the primary liable subject and the relationship with other

[718] Such as the *Schmitt* and *Allianz IARD* cases. "Elisabeth Schmitt v. TÜV Rheinland LGA Products GmbH, Case C-219/15," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/GA/ALL/?uri=CELEX:62015CJ0219.; "RB v. TÜV LGA Products GmbH and Allianz IARD S.A., Case C-518/18," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62018CJ0581.

[719] "Commission of the European Communities v French Republic, Case C-52/00," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62000CJ0052 (hereinafter Commission v France I); " Commission of the European Communities, Case, C- 177/04," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62004CJ0177 (hereinafter *Commission v France II*); "Societé Moteurs Dalkia Somer v Dalkia France and Ace Europe, Case C-285/08", EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62008CJ0285&qid=1659519214850 ; "Centre hôspitalier universitaire de Besançon v Thomas Dutreux and Caisse Primaire d'assurance maladie du Jura, case, C-495/10," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62010CJ0495 (hereinafter *Centre hôspitalier Besançon*).

[720] "N.W. and Others v. Sanofi Pasteur MSD SNC and Others, Case, C-621/15," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62015CJ0621&qid=1659519295161. (Hereinafter *Sanofi Pasteur*)

[721] *Commission v France I C-52/00* (judgment)

[722] *Commission v. France I C-52/00* (judgment)*Societé Moteurs Dalkia Somer,* C-285/08 (judgment)

[723] following "Cafpi SA and Aviva assurances SA v Enedis SA,Case C-691/21," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62021CJ0691. Hereinfter *Cafpi Aviva v Enedis.*

kinds of liability. Specifically in the *Schmitt* case, both AG Sharpston[724] and the CJEU mention it[725]. In the *Allianz IARD* judgment, the same kind of reasoning as in *Schmitt* appears: it concerns the primary liability of the producer in the PLD that does not have the obligation of taking out mandatory civil liability insurance. Moreover, in *Allianz IARD* the CJEU adds that the PLD does not seek to harmonise other systems of liability beyond the ones based on no-fault for products[726], a reminder that AG Bobek also makes in his opinion before the court judgment[727]. The two remaining cases concerning the PLD directly are extremely important: the first one, chronologically, *Novo Nordisk Pharma*[728], concerns the relationship between the PLD and a pre-existing, national liability regime for pharmaceutical products. The second case, *Boston Medezintechnik*[729] concerns the concept of potential defectiveness and damage to persons in high-risk products which are also medical devices, such as pacemakers and defibrillators.

Ex aequo with Germany, there is the UK, which was also the country (see Table 1) to actually have the first ever judgment before the CJEU regarding the PLD. This was an infringement procedure for "failure to comply" concerning the transposition of the risk development exception[730]. At a later stage, there were two judgments for a preliminary reference concerning vaccines (*O'Byrne* and *Aventis Pasteur*[731]) as defective products and the possibility for the plaintiff to substitute the defendant in the proceedings in order not to be time-barred. Moreover, the UK courts made an interesting referral inquiring about the status

[724] §32, In which AG Sharpston mentions that Article 3(1) PLD, read in conjunction with the second recital of the PLD, indicates that the producer manufacturer is the primarily liable subject. She also points out that despite the CJEU limiting the attempts of MS to extend the liability to the supplier easier, but at the same time has always indicated that the area of harmonization of the directive concerns no-fault liability. Hence, other regimes with more favourable outcomes for the consumers were implicitly allowed. "Opinion of Advocate General Eleanor Sharpston, delivered on 15 September 2016, Elisabeth Schmitt v. TÜV Rheinland LGA Products GmbH," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62015CC0219&qid=1659511812522.

[725] §58. The CJEU reminds us that Article 13 PLD "[…]*does not preclude the application of other systems of contractual and non-contractual liability based on other grounds such as fault*". *Schmitt* (judgment).

[726] §§ 41-42, *Allianz IARD* (judgment).

[727] §54, "Opinion of Advocate General Bobek, delivered on 6 February 2020, RB v. TÜV Rheinland LGA Products GmbH and Allianz IARD S.A.," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62018CC0581 .

[728] "Boston Scientific Medezintechnik GmbH v AOK Sachsen-Anhalt(503) v Betriebskrankenkasse RWE (504), Cases C-503/13, C-504/13," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62013CJ0503&qid=1659519999217 (hereinafter *Boston Medezintechnik*).

[729] "Novo Nordisk Pharma GmbH v S., Case, C-310/13," EUR-Lex, aAccessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62013CA0310&qid=1659520416126 (hereinafter *Novo Nordisk Pharma*).

[730] "Commission of the European Communities v United Kingdom of Great Britain and Northern Ireland, Case, C-300/95," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A61995CJ0300&qid=1659521422689 .(Hereinafter *Commission v UK*).

[731] "Declan O'Byrne v. Sanofi Pasteur MSD Ltd and Sanofi Pasteur SA, Case, C-127/04," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62004CJ0127&qid=1659521717510. Hereinafter *O'Byrne;* "Aventis Pasteur SA v. OB, Case C-358/08," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62008CJ0358&qid=1659521893152. Hereinafter *Aventis Pasteur*.

of software as a product in *The Software Incubator*[732] case, which was also peculiar as it was a judgment rendered after Brexit became effective (November 2021). It does not relate to the PLD but to the Directive 86/653 on commercial agents, but is important as it qualifies the perpetual licence of software in exchange for a periodical fee as "sale of goods", which might be useful with the IoT and their updates.

Afterwards, Denmark follows France in having all its three judgments exclusively about the PLD, with two very important preliminary references: *Henning Veedfald* [733]on physical damage and the exceptions for producers and *Skov Æg*[734], a judgment on the application of Article 3 PLD to suppliers, and, finally, one procedure for failure to comply with the obligations stated in the *Skov Æg* judgment[735].

Furthermore, Austria follows Denmark for number of judgments, but one judgment is about the application of the PLD in Private International law (*Kainz v. Pantherwerke*)[736] while the other is about whether the definition of false information as defective is correct (*Krone*[737]).

Greece and Spain each have one important judgment. Greece has one case issued by an infringement procedure for which it was sanctioned by the Commission[738]. This case is also important not only because it clarifies the relationship between the economic threshold of the PLD for property damage and denial of justice[739], but also because it mentions for the first time the relationship between Article 13 PLD and previously acquired rights by consumers under special liability regimes. This will turn out to be important as it is likely to be the basis for AG Szpunar's more recent and known *Novo Nordisk Pharma* opinion[740].

Spain has also had a very important preliminary reference case, *González Sánchez*, which clarified with *Commission v France I* and *Commission v Greece*

---

[732] "The Software incubator Ltd v Computer Associates (UK) Ltd , Case, C-410/19," EUR-Lex, aAccessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62019CJ0410&qid=1659522865512. Hereinafter *Software Incubator*.

[733] "Henning Veedfald v. Århus AmstKommune, Case, C-203/99," EUR-Lex, Accessed 31 January 2023 , https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A61999CJ0203&qid=1659524361571 (hereinafter *Henning Veedfald*).

[734] "Skov Æg v. Bilka Lavprisverehus A/S and Bilka Lavprisvarheus A/S v. Jette Mikkelsen and Michael Due Nielsen, Case C-402/03," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62003CJ0402&qid=1659528136269 (hereinafter *Skov Æg*)

[735] "Commission of the European Communities v Kingdom of Denmark, Case C-327/05," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62005CJ0327&qid=1659528164042 (hereinafter Commission v Danemark).

[736] "Andreas Kainz v Panterwerke AG, Case C-45/13," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62013CA0045&qid=1659528811811. Hereinafter *Kainz v Panterwerke*.

[737] "VI v. KRONE- Verlag Gesellschaft mbH &Co KG, Case C-65/20," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62020CA0065&qid=1659528863098. Hereinafter *Krone*.

[738] §§18-19, "Commission of the European Communities v Hellenic Republic, Case C-154/00," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62000CJ0154&qid=1659529345252. Hereinafter Commission v Greece.

[739] Article 9 (b)(i) PLD.

[740] §§30-31,"Opinion of Advocate General Szpunar, Novo Nordisk Pharma GmbH v S., Case, C-310/13," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62013CC0310.

the extent of the harmonization of the directive (maximum) and also the relationship of Article 13 PLD with other national product liability regimes and other contractual or fault-based systems[741].

Slovakia tried to make a preliminary reference procedure about the application of the PLD to legal persons, but it was later erased from the OJ[742]. Finally, Finland submitted its first request for preliminary reference on the PLD about how to identify a producer and the judgment was rendered recently (07 July 2022). In *Fennia v Philips*, the CJEU maintained that it is not the consumer's task to find the right producer when there are confusing situations, and it appears that there are two producers: the division of liability between these entities will be performed under the rules of Article 5 PLD. Moreover, in this judgment, it is stated that if someone presents themselves as producers, they must bear the risk to be considered as the actual producers and might be asked to pay for compensation and use a recovery action against the subject that they consider as the producer[743].

From a first quantitative and qualitative analysis, the hypothesis that I first advanced was confirmed: the more the pre-PLD system was favourable to the consumers, the more the country itself or its citizens challenged it in court (see supra 1.1.1, in particular France, Greece, Denmark and Spain had more protective rules for consumers prior to the PLD). In most of the infringement proceedings and preliminary references in the early 2000s, the CJEU did not admit that the national implementation of the PLD could follow a legal or procedural tradition of the MS. It rather argued that the discretion of the MS was established by the PLD itself and that any other national no-fault liability systems could not exist alongside the PLD, as the PLD was a maximum harmonization directive (although this expression never appears in the directive)[744]. Instead, Italy, which implemented the PLD as it was, because it did not have any previous *ad hoc* product liability legislation, did not have a single case (either preliminary reference procedure or infringement procedure) before the CJEU on the matter. This is also the same for Germany: the general rules of tort liability are likely to be used more than the PLD in Germany for normal consumer objects. One might then ask why, there were four cases from Germany. The reply is that one has to look at the types of the cases to understand this reasoning. The few cases that Germany had before the CJEU concerned the relationship with a special regime for pharmaceutical products (which was considered compliant with the PLD) in

[741]"María Victoria González Sánchez v. Medicina Asturiana, Case C-183/00," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3AC2002%2F180%2F08&qid=1659529978324. Hereinafter, *González Sánchez*.

[742] "Order of the President of the Court of 25 June 2013, (request for a preliminary ruling from Krajský súd v Prešove — Slovakia) — Spoločenstvo vlastníkov bytov MYJAVA v Podtatranská vodárenská prevádzková spoločnosť, a.s, Case C-496/12," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CB0496&qid=1659532663575.

[743] §§26-28, "Keskinäinen Vakuutusyhtiö Fennia v Koninklijke Philips N.V., Case C-264/21," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62021CJ0264&qid=1659530426486. Hereinafter *Fennia v Philips.*

[744] See §§38,47 *Commission v France I,* C-52/00; §§10,11,17, 18 *Commission v Greece* C-154/00; §§25, 29-31,*González Sánchez* C-183/00 and §§28, 34, 39 *Skov Æg* C-402/03.

Novo Nordisk Pharma, the potential defect of high-risks objects such as pacemakers and defibrillators in *Boston Medezintechnik* and the two cases involving the negligence of notified bodies (NB) and what the state could do in terms of compensation for victims, given that no rules from the PLD and the MDD could be applied regarding liability of the NB (*Schmitt and Allianz IARD*). There were either niche objects (pacemakers), residual issues (the special system of liability), or ones connected to the PLD which could not directly apply because of the context of the case[745]. Therefore, these judgments concern special, costly objects that were not the focus of the original projects of the directive or that, like in the cases of the defective prostheses, were part of an ad hoc regime, the MDD, ideally derived from the PLD.

2.2. Second quantitative and qualitative analysis: the EU PLD's most challenged articles

At this point, it is time to perform a quantitative and qualitative analysis of the PLD *stricto sensu*. As a methodological approach, I will use the database search results as before, but I will eliminate all the judgments that are not connected explicitly with the PLD (therefore Germany will lose two judgments from the database, Austria one and the UK one). The objective is to create a graph (Figure 3) that represents how many times the articles of the PLD (from 1 to 20) have been the object of preliminary reference or infringement procedures before the CJEU. This would prove useful in identifying the articles that will probably need a revision in the updated PLD, to make them more suited to domestic IoT technology.

[745] With regard to the defective breast prostheses cases, the PLD could not directly apply as the producer, PIP, had gone bankrupt.

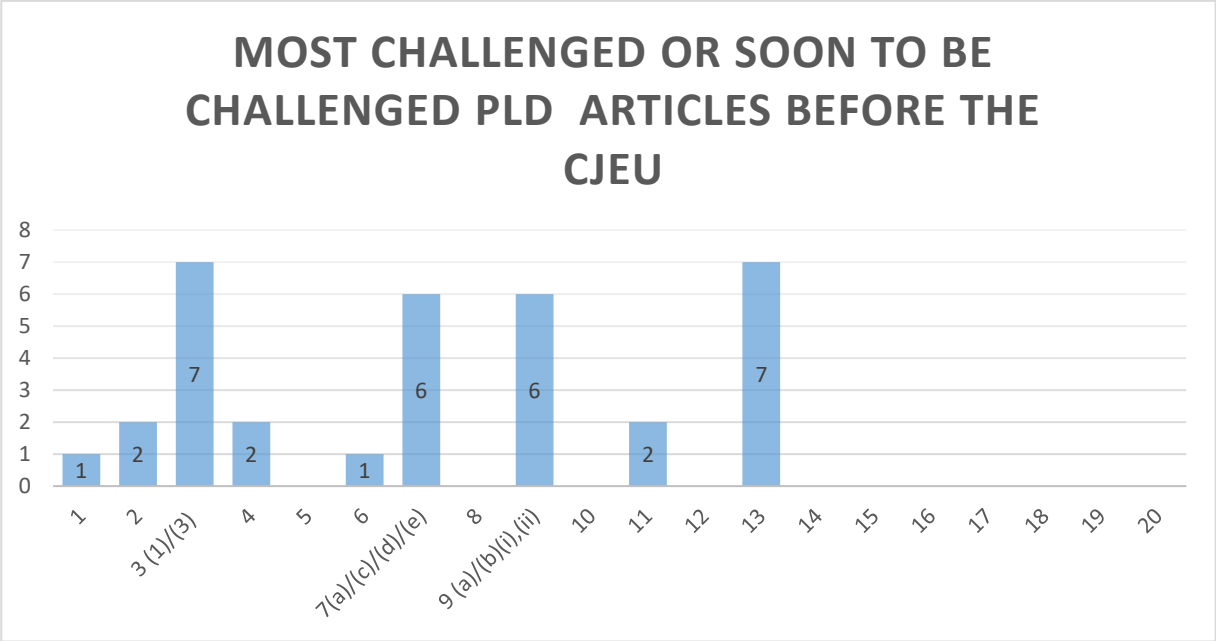

Figure 3

The quantitative analysis of the graph appears to be quite straightforward. The two most challenged articles in absolute terms were Article 3 (1)/(3) PLD[746], about the definition of producer, and Article 13 PLD, which concerns the PLD relationship with the MS systems of strict, contractual and fault liability[747]. Both articles occupy first place *ex aequo* on the podium of the most challenged PLD article as they were cited 7 times, and they were the main issue or one of the main issues of the concerned proceedings before the CJEU. It is quite likely that, if the texts of Article 3 PLD and 13 PLD remain the same, problems might also arise in the field of new technologies, as the distribution of competences has been more or less the same since 1985 in the Treaties. Considering the value- and supply- chain of the IoT, there is the risk that more confusion than before will arise with regard to finding the "right producer"[748].

Secondly, Article 9 PLD on the concept of damage is the most challenged both for its qualification of physical injuries[749] but also concerning the quantification of damage, and, more specifically, the cap of 500 euros in

[746] Respectively: 3(1) PLD: *Fennia v. Philips* C-264/21, and *Aviva* C-691/21; Article 3(3) PLD: *Commission v France I* C-52/00, Skov Æg C-402/03, *Commission v France II* C-177/04, *Commission v Denmark* C-327/05, and *Aventis Pasteur* C-358/08.
[747] *Commission v France I* C-52/00, *Commission v Greece* C-154/00, *Gónzalez Sánchez* C-183/00, *Skov Æg* C-402/03, *Société Moteurs Dalkia Somer* C-285/08, *Centre universitaire hôpitalier de Besançon* C-495/10 and *Novo Nordisk Pharma*, C-310/13.
[748] On these points see Chapter IV.
[749] Henning *Veedfald* C-203/99, *Boston Medezintechnik* C-503/13,C-504/13.

quantifiable damages[750]. This provision was challenged six times. Even in this case, the future PLD, if applied to new technologies, will have to take into account whether there might be a cap on damages and whether to include public in addition to private property, as well as mandatory insurance schemes. Second place *ex aequo* for the "mostly litigated PLD article" goes to Article 7 PLD, on the exceptions to the application of the PLD that the producer can use. This was questioned six times. The mostly litigated exceptions are the risk development exception, of letter e) (2 cases[751]) and the letter a) exception, based on the fact that the producer did not put the product into circulation (2 cases)[752]. Then also letter c) [753] and d) were discussed once[754].

With two judgments each, there are Articles 2, 4 and 11 PLD, respectively on the definition of product[755], the defendant's burden of proof relating to the damage (meaning the damage, the causal link and the relationship between defect and damage)[756] and the ten-year limit for producers' liability[757]. And, finally, there is Article 6, concerning the defectiveness of the product and Article 1 PLD, concerning the scope of the PLD with just one case[758].

From a qualitative point of view, Figure 3 also has to be interpreted by taking into account the history and the evolution of the PLD over 30 years. It is undeniable that the two most important trends concern the division of competence of liability and the subjects that can be assimilated to or could be the producer (such as the supplier or the distributor). However, I argue that the most important of these two trends is indeed the one concerning the division of competence between the MS and the EU, which is represented by Article 13 PLD about the relationship with the PLD and other forms of national liability. In fact, France, Denmark or Greece would not have inserted the rules concerning the equivalence between supplier and producer/manufacturer if, on the basis of Article 13 PLD, they had not considered that they had competence and a duty to implement the PLD in a manner that they believed convenient for the consumer. Historically, the CJEU dealt with the problem of the division of competence in two phases.

The first historical period goes from the year 2000 to 2004 during which the core rules (which are valid until now) about the PLD and other national liability systems were defined. In this period, the judgments *France v Commission I and II, Greece v Commission, Gónzalez Sánchez, Skov Æ*g and *Commission v Denmark* established the following points. Firstly, that the PLD was a maximum

[750] Such as in *Veedfald Commission v. France I* C-52/00, and *Commission v. Greece* C-154/00, *Société Moteurs Dalkia Somer* C-285/08.
[751] *Commission v. Uk* C-300/95, and *Commission v. France* C-52/00.
[752] *Henning Veedfald* C-203/99, *O'Byrne* C-127/04.
[753] *Henning Veedfald* C-203/99.
[754] *Commission v France I* C-52/00.
[755] *Krone* C-65/20 and the pending case *Aviva* C-691/21.
[756] *Novo Nordisk Pharma* C-310/13 and *Sanofi Pasteur* C-621/15.
[757] *O' Byrne* C-127/04 *Aventis Pasteur* C-358/08.
[758] It is in both cases *Boston Medezintechnik*. As they are joined cases, I considered them as just one. *Boston Medezintechnik* C-503/13, C-504/13.

harmonization directive[759]. Secondly, with the PLD being a maximum harmonization directive, it was necessary that the national implementation strategies needed to be respectful of its scope, even when the MS were allowed a margin of discretion as far as the application of the same directive was concerned[760]. The respect of legal traditions and legal habits which favoured consumers more when it came to defective products and that were also based on a no-fault scheme could not co-exist alongside the PLD[761]. In fact, if a special regime of liability, even one not based on fault, was limited to certain products, it could be compatible with the PLD[762]. Moreover, the PLD did not preclude the MS from having contractual or fault-based systems or special liability regimes which tackled the aspects that the PLD did not seek to harmonise (such as procedural law). The fact that all these judgments were close in time made it possible to ensure high coherence as the AG was the same for all of these cases, namely AG Geelhoed. Most probably, Geelhoed followed a historical approach (already illustrated by Tesauro in its opinion in *Commission v UK*[763]) concerning the origin of the PLD, which was the result of a long process of negotiation and eventually of compromise[764]. Also, in a systematic interpretation of the Directive, the fact that consumer protection was mentioned in one of its recitals did not mean that it had to prevail over the legal basis on which the PLD was founded, meaning Article 100 TEC, (then 94 EC and now 114 TFEU) which concerns the harmonization of the market and has a regulatory nature. The same CJEU stated that it was not possible to interpret the PLD in the light of then Article 153 (the clause on consumer protection, now 169 TFEU) retroactively[765]: as a matter of fact, when the PLD was approved, there was no clause on consumer protection in the Treaties, just one regarding harmonization[766].

This "hard" line passed (and, in fact, after 2003 the issues with Article 13 become less frequent[767]) and was consolidated both in later opinions of AG Mengozzi, Szpunar, Trstenjak and Bobek, who all made reference to that group of cases from the beginning of the 2000s, and also in the court judgments. The only exception and outright opposition to this trend of limiting application of the PLD to the harmonization clause was the Opinion of AG Bot in the *Boston*

[759] § 46 "Joined Opinion of AG Geelhoed delivered on 18 September 2001, Commission of the European Communities v French Republic, María González Sánchez v Medecina Asturiana," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX:62000CC0052, hereinafter Opinion *France v Commission I* and *González Sánchez* .
[760] §§22-25 *Commission v France I* C-52/00; §25, and §§29-31 *González Sánchez* C-183/00; §10 *Commission v. Greece* C-154/00.
[761] §38 *Commission v France I* C-52/00 and 39 *Skov ÆG* C-402/33.
[762] §§ 17-19 *Commission v Greece*, §39 Skov Æg C-402/33.
[763] §§15-19 "Opinion of Advocate General Tesauro Commission of the European Communities v United Kingdom of Great Britain and Northern Ireland, Case C-300/95," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX:61995CC0300.
[764] Simon Whittaker, "The Creation and Maintenance of the EEC Directive on Liability for Defective Products and the Process of its Implementation in the UK and France," in *Liability for Products: English Law, French Law, and European Harmonization*, Simon Whittaker (Oxford: Oxford University Press),436.
[765] §§10-11 *Commission v Greece* C-154/00.
[766] Simon Whittaker, "The Creation and Maintenance of the EEC Directive on Liability for Defective Products and the Process of its Implementation in the UK and France," in *Liability for Products: English Law, French Law, and European Harmonization*, Simon Whittaker (Oxford : Oxford University Press), 430-475.
[767] See the column with the Articles involved in the judgments schematised in Table 1 of this chapter.

Medizintechnik cases of 2014. He explicitly relied on the second recital of the PLD on consumer protection in order to interpret the concept of safety that the consumer was entitled to expect[768]. In his reasoning, AG Bot was relying more on securing consumer protection after, as he stated, the increasing number of health scandals regarding the implantation of medical devices[769] blatantly contradicted the EU purpose of always aiming at *"…integrating human health protection requirements* […] *into all Union policies*"[770]. Contrary to what Geelhoed thought was the regulatory mission of the PLD, Bot instead maintained that it was possible and indeed necessary to interpret the PLD by bearing in mind the policy favouring the protection of consumers' safety expectations. Even if the PLD had been adopted under Article 100 EEC, this did not mean that the harmonising measures adopted by relying on it "[…] *did not have an objective of guaranteeing consumer protection*"[771]. The position of AG Bot, who was a former French magistrate, could also be understood not only from his explicit mentions of health scandals from previous years but also by analysing those aspects of French legal culture that have always been more victim-oriented (*la victimologie*) and on the precautionary principles that a modern welfare state (the *État-Providence*) adopts. Moreover, France was also the MS which was fined most for its delay and "incorrect" transposition of the directive[772], together with Greece and Denmark. These states, so different from each other in terms of legal traditions, shared the same focus on protecting consumers. France also had the highest absolute number of cases discussed directly that concerned the PLD. Therefore, it makes sense that the French AG's opinion on the matter was different compared to his colleagues' views on the subject.

Chronologically, AG Bot's positions integrate a second part of the timeline considered and indeed, they are an exception in the series of judgments concerning the PLD. The second part of the timeline starts from 2004, the year of the last opinion by AG Geelhoed in *O' Byrne* and consists of two main sub-trends: on the one hand is a less interesting one, which again concerns Article 13 PLD but affirms the previous jurisprudence 2000-2003 such as in *Société Moteurs Dalkia Somer* and *Centre hôpitalier de Besançon*. The other sub-trend started with *O'Byrne* and continued with *Aventis Pasteur*, *Novo Nordisk Pharma* and *Sanofi Aventis*. These judgments concern national courts asking how national substantive and procedural rules that are connected to a greater or lesser extent to the PLD interact with the PLD itself. At a first glance, the impression is that both the AGs and the CJEU were becoming more tolerant,

[768] §30: "…[the] concept of "safety which a person is entitled to expect is relatively imprecise…Interpreted in the light of the objective, set-out in the second recital… that concept must be understood to refer to a product that poses risks jeopardising the safety of its user and having an abnormal unreasonable character exceeding the normal risks inherent to its use". Opinion of Advocate General Bot, *Boston Scientific Medizintechnik GmbH v AOK Sachsen-Anhalt – Die Gesundheitskasse* and Betriebskrankenkasse RWE, Joined Cases C-503/14 and C-504/13," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62013CC0503&qid=1659555918695. Hereinafter, *AG Bot opinion Bostonmedezintechnik*.

[769] §73 *AG Bot opinion Bostonmedezintechnik.*

[770] §41 *AG Bot opinion Bostonmedezintechnik.*

[771] §39 *AG Bot opinion Bostonmedezintechnik*.

[772] France had two infringement proceedings for failure to comply: *Commission v France I*. C-52/00 and also *Commission v France II* C-177/04.

allowing (in general) the national courts to take initiative, which, in turn, seemed less defiant of (or maybe they were resigned to) the maximum harmonization character of the PLD. Probably, national judges just wanted to understand whether their substantial or procedural rules were compatible with the directive, or, how they could adapt them to the EU instrument, given that the PLD was silent on the matter especially with reference to the latter ones.

Some signs of a less tense relationship between the CJEU and the national courts, go back to the early decisions of the Court. Remember, for instance, that in the *O'Byrne* case AG Geelhoed allowed the MS to interpret Article 11 PLD on the liability of the producer more favourably to the consumer/patient. This was done to avoid holding the plaintiff to be time-barred because of the bad faith of the producer[773]. Furthermore, in *Aventis Pasteur*, AG Trstenjak stated that the directive had both consumer protection, competition and movement of goods as its objectives[774]. Nevertheless, in the same opinion, AG Trstenjak clearly stated that the UK procedural rule, which operated an automatic substitution of the producer with another subject involved in the manufacture of the product (in that case a vaccine) in order for the plaintiff not to be time-barred after 10 years had passed, was indeed contrary to the directive[775]. This meant that the PLD was still a maximum harmonization instrument and that Article 11 PLD needed to be interpreted bearing in mind all the case law on Article 13 PLD. This ambivalence between protective instances towards consumers/patients and the maximum harmonization character of the PLD is present also in *Novo Nordisk Pharma*. The Court, following AG Szpunar's opinion[776], considered that a special German regime of liability for pharmaceutical products was compatible with Article 13 PLD as the directive did not attack the previously acquired rights of the German people[777]. However, the opinion and the judgment differ on one point. The case involved access to medical documentation on the side-effects of a drug taken for diabetes. The referring court had asked the CJEU whether Article 4 PLD could cover the request to access the information relating to medical products even if not covered by a special liability regime. AG Szpunar was in favour of such an interpretation (which in the case of adverse medical effects could prove helpful to plaintiffs) also because he claimed that, despite the German pharmaceutical product liability system being excluded by the application of the PLD, this did not mean that it could not be influenced by the harmonising effects of the PLD itself[778]. The CJEU clearly opposed this view[779]: it considered the two

[773] §65: "[…] it is not contrary to the Directive, in particular to Articles 3(3) and 11, to permit the court seised of a claim brought by a plaintiff against the producer when the supplier knew who the producer was and could have informed the plaintiff". Opinion of Advocate General Geelhoed Declan O'Byrne v Sanofi Pasteur MSD Ltd and Sanofi Pasteur SA," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A62004CC0127. Hereinafter *O'Byrne Opinion*.
[774] §75 "Opinion of Advocate General Trstenjak, Aventis Pasteur SA v OB. Case C-358/08," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62008CC0358. Hereinafter *Opinion Trstenjak , Aventis Pasteur*.
[775] §80 *OpinionTrstenjak Aventis Pasteur*.
[776] "Opinion of Advocate General Szpunar Novo Nordisk Pharma GmbH v S, Case C-310/13" EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62013CC0310. Hereinafter *Opinion AG Szpunar Novo Nordisk Pharma*.
[777] §30-34, *Opinion AG Szpunar Novo Nordisk Pharma;* §§20-21,31, *Novo Nordisk Pharma* C- 310/13.
[778] §36, §47, *Opinion AG Szpunar Novo Nordisk Pharma*.
[779] §25, *Novo Nordisk Pharma* C- 310/13.

liability schemes as separate and if the German system was allowing a mechanism to get hold of information to prove damage, the impact of this national liability system was in any case not harming an effective application of the PLD[780]. In *Sanofi Aventis*, AG Bobek[781] and the CJEU[782] gave the referring court, the French *Cour de Cassation*, a list of guidelines about which principles the national court had to comply with in order to be compliant with Article 4 PLD. While acknowledging that the standard of proof was not harmonised by the PLD, AG Bobek also maintained that the MS had to respect the principle of equivalence and effectiveness while implementing national rules on the standard of proof[783]. Also, the directive does not require proof through scientific causation[784] but what national procedure rules must do is to avoid rules on proof that "[…] *explicitly prohibit judges from taking potentially relevant evidence into account or identify specific pieces of evidence as systematically constituting conclusive and non-rebuttable evidence of a given fact* […][785]. The reasoning of the Court aligns with the AG's opinion[786], but, at the end, it also gives an evaluation of the procedural rules in place, in particular to the ones governing legal presumptions to demonstrate causality in difficult cases, such as medical side-effects. The Court states that the French national evidentiary rules are neutral regarding the burden of proof of Article 4 and "[…] *are in principle capable of preserving the effectiveness of the system of liability provided for* […]" by the PLD[787]. In any case, an evaluation of these rules must be performed by taking into account the habits of application and interpretation given by national courts. Courts can be extremely rigorous or, conversely, they might create an immediate and automatic presumption "where one or more types of factual evidence were presented together"[788]. The solution to this conundrum is that "[…] *the national courts must first ensure that the evidence adduced is sufficiently serious, specific and consistent to warrant the conclusion that, notwithstanding the evidence produced and the arguments put forward by the producer, a defect in the product appears to be the most plausible explanation for the damage, with the result that the defect and the defect and the causal link may reasonably be established*"[789].

To sum up, despite the issues in interpreting Article 13 PLD and, in general, the division of competence between the EU and the MS, no longer concerning the relationship with other national liability schemes (how the CJEU sees the matter is pretty clear), the analysis of more recent judgments shows that the source of legal uncertainty in the application of the PLD increasingly regards national procedural rules. These rules are formally outside the PLD scope of application but, nevertheless are touched by the PLD harmonising effect. I

[780] §26-32, *Novo Nordisk Pharma* C- 310/13.
[781] "Opinion of Advocate General Bobek, N.W. and Others v Sanofi Pasteur MSD SNC and Others, Case C-621/15," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62015CC0621. Hereinafter *Opinion of Advocate General Bobek Sanofi Pasteur*.
[782] *Sanofi Aventis* C-621/15.
[783] §§ 16-24, *Opinion of Advocate General Bobek Sanofi Pasteur*.
[784] §§42-44, *Opinion of Advocate General Bobek Sanofi Pasteur*.
[785] §45, *Opinion of Advocate General Bobek Sanofi Pasteur.*
[786] §22-24, *Sanofi Aventis* C-621/15.
[787] §33, *Sanofi Aventis* C-621/15.
[788] §§34-36, *Sanofi Aventis* C-621/15.
[789] §37, *Sanofi Aventis* C-621/15.

believe these issues should increase in frequency with the gradual application of the PLD and its update to new technologies.

3. The future PLD and its interaction with other legislative and policy documents.

This section is a bridge between the past and the present of the PLD. The findings of the survey on CJEU case law concerning product liability led to the compiling of a list of the PLD articles that will need to be modified to make this legislative act fit for new technologies such as low-risk technologies (e.g., IoT for the home). I will therefore select some of the articles that were challenged the most and then some others which, despite not being discussed much before the court, may be a source of litigation when it comes to new technologies. That is why in the following subsections I will deal with Articles 2, 3, 4, 6 7, 9, 11 and 13 by giving inputs for a future PLD. In order to advance ideas for the reform of the PLD, there are some elements to consider in a preliminary way. At the moment of writing, an official updated draft of the new PLD is not available[790]. There are some academic projects involving a complete redraft of the PLD, such as the one of the European Law Institute (ELI), but no official documents yet[791]. This is perhaps for the best, as there is more room to speculate about what the future PLD should look like. In order to do that, I will use legislative and policy acts from the EU. There are four important documents that I will focus on: the directive EU/2019/771 on the Sale of Goods (we will focus on the goods with interconnected software hence Sale of Digital Goods, SDG), and its "twin", the Directive EU/2019/770 on the Supply of Digital Content and Digital Services (DCDS). As it is known from Chapter III, they are important because they are the first legislative acts in European Private Law which regulate IoT objects, even without mentioning them. There is also the GDPR, which is important because of the centrality of personal data processing by IoT home objects. Finally, there is the proposed Data Act (DA), as it tries to give to users (be they consumers or professionals) the possibility to have better control by accessing and using the data produced by their own IoT objects. Nevertheless, it is also important to include the already commented EG report on the liability of AI and new technologies in the analysis. This report was already described in chapter III and it is from this that we derive the arguable difference between high-risk AI applications (which should follow a strict liability model) and low-risk AI applications, whose rules of liability should be the ones of tort/extra-contractual liability. While I still disagree with the view of the EG[792] that objects to domestic IoT responding solely to fault (tort or extra-contractual) liability, as they are

[790] At the moment of writing, meaning 13 August 2022.
[791] "Reform of the Product Liability Directive," ELI website, Accessed 31 January 2023, https://europeanlawinstitute.eu/projects-publications/current-projects/current-projects/pld/.
[792] Expert Group on Liability and New Technologies. *Liability for Artificial Intelligence Report from the Expert Group on Liability and New Technologies-New Technologies Formation*. Brussels: European Commission, 2019, Accessed 31 January 2023. https://op.europa.eu/en/publication-detail/-/publication/1c5e30be-1197-11ea-8c1f-01aa75ed71a1/language-en.

considered generally “low risk”’, I take in consideration this document as it offers interesting perspectives and provides practical solutions on how to make it less difficult for plaintiffs to prove damage caused by technology. Moreover, in this analysis there will be references to the most recent ELI’s response to the EU Commission’s public consultation to adapt civil law rules to the digital age (hereinafter ELI response[793]), as it is a document that is also rich and full of insights. It thoroughly describes the connections of the future PLD with existing EU law. Finally, there will also be a comparison with the views of Insurance Europe, the European group of interests which represents the interests of insurances companies in Europe (hereinafter Insurance Europe report)[794] which also responded to the same public consultation the ELI responded to. This document is important, as PLD is not only an instrument of harmonization of the market, until now, but also due to the allocation of risks that the producers have to analyse and to prevent in advance through the use of insurance contracts.

3.1.1. Future Article 2 PLD

When thinking of the possible evolution of Article 2 PLD, which describes the field of application of the directive (what is considered to be a product), as in the proposed PLD, the EU legislative documents that come to mind as models for the update are the SDG and the DCDS. The SDG and DCDS have one main area of overlap: goods with digital elements, which are respectively cited in Article 2(5)(b)SDG and Article 2(3)DSCD. The goods with digital elements in both definitions are characterised by two distinctive features. The first one is that they are interconnected, or incorporate digital contents or digital services. The second one is that the lack of those contents and services makes it impossible for the object to perform its functions. This will influence the drafting of the new Article 2 concerning the field of application of the PLD[795]. Most probably it would be an added comma mentioning the definition of a good with digital element and also the definitions of digital content and digital services that may be found in Articles 2(6) and 2(7) SDG. This would also mean that, aside from the use of the term “incorporated”, the term “interconnected” must also be mentioned, that constitutes a new way of functioning for these objects. One might also wonder why the definition of product that we find in Article 2(2) of the Data Act[796] cannot be applied. It might be clearer when looking at the definition of what an IoT object

[793] Bernard Koch, J. Borghetti, P. Machinowski et al., “Response of the European Law Institute Public Consultation on Civil Liability: Adapting liability rules to the digital age and artificial intelligence, ” (2022) Accessed 31 January 2023, https://europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Response_to_Public_Consultation_on_Civil_Liability.pdf.Hereinafter ELI response (2022).

[794] Áine Clarke, “ Adapting liability rules to the digital age and artificial intelligence,” *Insurance Europe*, 16 February 2021,aAccessed 31 January 2023 https://www.insuranceeurope.eu/mediaitem/46c3d081-6db4-4d62-af388b356591f3dc/Adapting%20liability%20rules%20to%20the%20digital%20age%20and%20artificial%20intelligence.pdf. Hereinafter Insurance Europe report.

[795] ELI response (2022), 8.

[796] Article 2(2) DA recites as follows “[…]‘*product’ means a tangible, movable item, including where incorporated in an immovable item, that obtains, generates or collects, data concerning its use or environment, and that is able to communicate data via a publicly available electronic communications service and whose primary function is not the storing and processing of data*”.

is, especially the ones that are meant to be in the home. Nevertheless, I believe it is more practical to provide a layered definition of product (by mentioning its interconnectedness and it being able to incorporate digital content). This is because, as much as one would wish it didn't exist, there is still a legal division between the regime of services and goods in the internal market. Having a more faceted definition of products also allows us to take into consideration other hypotheses that are quite common in our interaction with low-risk AI applications, such as IoT for consumers. This definition provides for the theory that services such as data in form of content (such as app downloaded on the device), or Software as a Service (SaaS) should be taken into consideration by the PLD. The ELI response suggests including both digital data and the software as a service in the application field of the PLD, not to weigh all the liability on the producer/ manufacturer, but on the operator/ programmer/creator of the standalone data or the owner of software as a service[797]. It seems only fair not to weigh all the burden of product liability on the manufacturer of the product, especially when there could not be a contractual relationship between the IoT producer and the SaaS developer. This might occur, for instance, because the SaaS service or app was not pre-installed on the device, and it was only the consumer/user's choice to download it. This allocation of liability would also reflect the actual reality of IoT technology at present and also be compatible with the evaluation of licensed software as a good, hence a product, as suggested by the *Software incubator* judgment[798]. As explained in Chapter II, a fault in data processing can cause damage (involving both non personal and personal data) but it may also elsewhere, other than in the device. As the Commission Staff Working Document accompanying the Final report on the sector inquiry into consumer IoT explains, apart from the device, processing can happen "[…] *in a companion app on a smart mobile device, (iii) in third-party cloud services providers' processing infrastructure ("in the cloud") and (iv) in company owned infrastructure*"[799]. However, at the moment, the IoT for the home rarely has enough computational power *in situ*: edge applications on IoT devices[800] are still in a minority while most data processing activities take part in the cloud or in servers elsewhere.

Neither the ELI response, nor the Insurance Europe report mention what happens when technological standards are faulty, and how to connect them with product liability. In Chapter IV, there was a subparagraph[801] dealing with the state of harmonization of tort liability and the role of international standard setting organisations (SSOs) and standard development organisations (SDOs). To be concise, if the standard is international and not integrated within a national implementing act, only MS tort (or in some cases contractual) liability remedies could work. If, instead, as prompted by the new Data Act, there are harmonised

[797] ELI response (2022), 11-12.
[798] §32, *Software incubator* C-410/19.
[799] Commission Staff Working Document. Accompanying the document REPORT FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT Final-Report- Sector inquiry into consumer Internet of Things (COM(2022)19 final) , Brussels, 20.1 2022, SWD(2022) 10 final, 89. Accessed 31 January 2023, https://competition-policy.ec.europa.eu/system/files/2022-01/internet-of-things_final_report_2022_staff_working_document_0.pdf.
[800] Edge technology means to increase the computational power at the edge of the cloud system, hence, most of the times, directly in the object. See Chapter II.
[801] 1.1.2., I, Chapter IV.

standards, users/consumers can in principle bring proceedings before the CJEU, either indirectly through a preliminary reference made by a national court (Article 267 TFEU), or directly, by relying on the fact that the EU is liable under contractual and non-contractual liability (Article 340 TFEU). However, an individual reference to the CJEU has been denied many times in the past[802]. It would be better if the SSO and SDOs under harmonised standards could be made liable with the other subjects (producer-manufacturer; trader/operator of external services) on a stand-alone basis, depending on what the cause of the damage was.

Moreover, as neither the SDG nor the DCDS explicitly mention whether they apply to refurbished technological goods, the new PLD should make it explicit that it applies to the producers of refurbished goods. In fact, the refurbishment procedure is more invasive than just acquiring a second-hand object, as it allows elements of the connected object to be changed. This position is shared both by the ELI response and by the Insurance Europe report[803]. If the EU wishes to favour more sustainable technological solutions for consumers/users, then it has to make sure that there are not liability loopholes.

Regarding incorrect information, quite a recent case of the CJEU (*Krone*[804]) established that incorrect health information (in a magazine) leading to physical damages should not be considered as a defective product. The main reason why information could not make an object defective is because goods and services have two different disciplines and information is not a tangible product[805]. Despite the fact that this approach is understandable and acceptable when discussing traditional non-connected objects, I am not sure this reasoning will hold when there is an interactive relationship between a human and an IoT object for the home. In connected objects the information delivered might be dangerous if the addressee is a person who is vulnerable because of their age (especially children). The case of an English child asking Alexa what they can play and Alexa replying they should insert a coin in an electric socket might have been a tragedy if the child had complied with the object's instruction[806]. In that case, there was no printed text, but it might be impossible to think that the display of an IoT object could provide incorrect information. As recalled in Chapter IV, there are more and more reports of domestic accidents caused by the use of augmented reality visors. In these cases, the visor collects and processes environment data in an incorrect way and the person can only trust the data, which becomes faulty information[807]. In the *Krone* judgment, the Court does not provide clear

[802] See the reference to the *Plaumann* judgement, chapter IV.
[803] Bernard A. Koch et al., *Response of the European Law Institute Public Consultation on Civil Liability Adapting liability rules to the digital age and artificial intelligence* (Wien; ELI, 2022) (document already cited) 13.
[804] § 30 "Opinion of Advocate General Hogan VI v. KRONE- Verlag Gesellschaft mbH &Co KG, case C-65/20," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62020CJ0065 . Hereinafter *Opinion of Advocate General Hogan VI v. KRONE.*
[805] §§ 37-39 *Krone C-65/20* (Judgment).
[806] BBC News Tech, "Alexa tells a 10-year-old girl to touch live plug with penny," 28 December 2021, Accessed 31 January 2023. https://www.bbc.com/news/technology-59810383.
[807] Jem Bartholomew," Rising popularity of VR headsets sparks 31% rise in insurance claims," *The Guardian*, February 12, 2022, https://www.theguardian.com/technology/2022/feb/12/rising-popularity-of-vr-headsets-sparks-31-rise-in-insurance-claims .

indications of what would happen in these cases, but it does provide some guidance. The CJEU states that one should consider a product as defective by considering the inherent characteristics of the product; therefore, it is important to distinguish between the information carriers, which just relay information, and those which use information to function and perform[808]. This discussion, however, leads directly to the question of whether the solution of having the manufacturer of the object as the only producer, eventually substituted by other subjects if its identity is unknown, is still the best idea when it comes to new technologies. These issues concerning the identity of the producer and its relationship with the supply and value chain of IoT objects (domestic one included) will be dealt with in the subsequent paragraph.

3.1.2. Future Article 3 PLD

The current structure of Article 3 PLD leads us to think that there must only be one person who is liable: the producer, who is also understood to be the manufacturer of the finished product, or, in any case, anyone who presents themselves as the producer can effectively be considered as such, and, therefore, be liable[809]. However, the second paragraph of the same article also includes the importer, without prejudice to the producer. Article 3(3) PLD instead, in order to avoid liability loopholes, states that the supplier of the product shall be treated as the producer unless it informs the victim of the true identity of the producer. In this way, the PLD creates what AG Trstenjak calls the "functional producer"[810] The supplier is not defined by the directive, hence, according to AG Mengozzi, it should be considered as an intermediary[811].

According to the CJEU case law, however, this does not mean that the plaintiff has a direct action against the supplier itself. Many MS, such as France and Denmark in particular, did not accept this idea because of their legal traditions on the matter, and tried to implement Article 3 PLD in their own way. This was opposed by the Court in the *Skov Æg* case[812], but also in *Commission v France I*[813]. The CJEU sanctioned a country which had transposed its internal rules on recovery action from the supplier to the producer in one case (France); in the other case (Denmark), the CJEU answered the questions of the judges on the compatibility of the Danish no-fault liability system with the directive. In the first case, France had changed the text of Article 3 PLD to make the supplier as liable as the producer, while Article 3(1) and (3) PLD did not allow this. Although the supplier still had the possibility to act retroactively to recover the sum of money paid to the consumer from the producer, the CJEU did not justify that the French legal tradition was actually the reason why this rule was changed[814].

[808]Piotr Machnikowski, "Product Liability for Information products?: The CJEU Judgment in VI / KRONE - Verlag Gesellschaft mbH & Co KG, 10 June 2021 [C-65/20]," *European Review of Private Law* 1(2022):200.
[809] Article 3(1) PLD. In this case, the recent preliminary reference made by the Finnish court on the identity of the producer could have a easy response. See Table 1 C-264/21.
[810] §§34-39 Opinion AG Trstjenak *Sanofi Aventis*.
[811] Fairgrieve Duncan et al. "Product Liability Directive," in *European Product Liability: An Analysis of the State of the Art in the Era of New Technologies*, Piotr Machnikowski (Antwerp, Cambridge, Portland: Intersentia 2016), 68.
[812] *Skov Æg* C-402/03.
[813] *Commission v France I* C-52/00.
[814] §38 *Commission v France I.*

Similarly, the same happened with *Skov Aeg*, where it did not matter whether there was a national no-fault liability rule for the supplier: the supplier could not be considered liable if it was clear who the producer was. Given that the PLD was of maximum harmonization (see infra the paragraph on Future Article 13 PLD), this kind of liability was incompatible with the margin of discretion given to the MS by the same PLD[815].

Even though it was clarified many times that primarily allocating product liability on one subject (the producer-manufacturer) was done to help consumers and to reduce the number of complaints, it is still difficult for consumers to really understand who the producer is, especially when dealing with an IoT object supply chain. Despite this situation, things might be slowly changing on this issue, even for the CJEU. An example of this could be the recent case *Fennia v Philips*[816]*.* In *Fennia v Philips,* a defective coffee machine caused a house fire. The defective product had trademarks and distinctive signs from both Philips, the main company, and Saeco, the actual manufacturer that materially built the machine. When the insurance company Fennia asked Philips to pay compensation for the consumer's house insurance policy, Philips refused, saying that the producer was Saeco, not Philips. In response to this problem the CJEU stated that the interpretation of Article 3(1) PLD and following paragraphs did not leave space for any doubt that whoever presents themselves as a producer is not, solely for that reason, comparable to the producer itself[817]. Nevertheless, the CJEU clarified that through Article 5, the PLD provides for any entity presenting itself as a producer to have to take the chance that the consumer might expect compensation in full from them, as Article 5 PLD claims that there can be more than one producer that are liable jointly and severally[818]. Following this comprehensive interpretation, Article 3 PLD is a facilitator for consumers as they will not have "[…] *to determine the actual producer of the defective product in question.*"[819] In the case at hand, Philips, which was substantially the producer as it owned the trademark of Saeco, and had received the request for compensation from Fennia insurance on behalf of the consumer, was forced to pay. This judgment is particularly interesting for two reasons: for the first time the CJEU acknowledges indirectly that there might be problems in identifying the producer-manufacturer not only in specific and complex cases, such as the ones involving vaccines and medical products[820], but also for consumer objects. From the judgment, it is not possible to infer whether the coffee machine was a smart coffee machine, but it is probable. Hence it promoted a teleological reading of Articles 3 and 5 PLD justifying consumers who are led to believe that a subject is as much a producer as another. Could it be an implicit reversal of all the judgments which saw the supplier as not an immediate substitute of the producer? I do not think so, but I believe that the combined reading of Articles 3 and 5 PLD could help in making more subjects accountable in an IoT product liability context. Paragraphs (4) and (5) of Article 82 GDPR establish that the data

[815] §§ 31- 45 *Skov Æg*.
[816] *Fennia v Philips*, C-264/21.
[817] § 27, *Fennia v Philips*, C-264/21.
[818] §32, *Fennia v Philips*, C-264/21.
[819] §33 *Fennia v Philips*, C-264/21.
[820] See *O'Byrne* and *Aventis Pasteur* in subparagraph on Article 11 perspective PLD.

subject who endured a violation according to Data Protection rules could ask for compensation from both the controller(s) and the processor(s) that caused the violation. The issue of how these subjects can recover the damages paid to the data subject is an issue for national laws to regulate, most likely through a series of recovery actions.

In any case, the issue of the producer has not been clearly solved: the fact that the two recent CJEU cases, *Fennia v Philps* and *Cafpi Aviva v Enedis*, dealt with issues on how to identify the producer means that the debate is still open. It is therefore a sign that the PLD rule is not fully accepted by the MS and I believe that this needs to be modified, at least for the domestic IoT, whose chain of production is far more complex, as it is only possible to understand clearly who the actual producer is in very few cases[821]. I think it is important to move away from the traditional point that there must only be one producer that coincides with the manufacturer, because, with connected objects, this is simply no longer true. If we consider standalone software as a product, its producer may not be the manufacturer of the object or be connected with it through contractual relations as already stated in the previous subparagraph.

In fact, sometimes the producer-manufacturer of the physical object is not even bound by contractual relationships (such as for standards). Or, if it is, it may be contractually bound to an international provider of services or company, which sets the contract in its own favour. At the moment, it is still unclear how the Data Act's rules of Article 13 will be applied in cases such as the one presented. This article states that any clause limiting remedies and availability in data sharing contracts will be considered invalid[822]. However, to be applied, the party that must comply with the unfair contractual clause(s) must be a small-medium enterprise, in accordance with EU law. It would be advisable to abolish the "one producer only" idea, and, provided that the factual situation is analysed in depth, to consider whether the role of the producer could be "functionally accomplished", as Trstjenak would say, by the trader or vendor (in the language of the DCDS or SDG) or the data holder (in the DA) whenever the damage comes from the service or content that the IoT presents to the consumer-user. Alternatively, the producer could coincide with the GDPR controller or processor when the PLD damage is caused by faulty data processing.

This need to establish a first point of contact that the consumer can access easier than the remote (and maybe outside the EU) producer is not without previous examples, especially in EU Data Law and in medical regulation. For example, the GDPR and the Data Act provide for points of contact whether the company interested in personal data processing or data sharing are European companies or not[823]. The ELI also shares this position and states that we must take inspiration from other documents that create a hierarchy with

[821] Just the model 1 which is typical of the main global producers of IoT, such as voice assistants. See Chapter IV.
[822] 13(3) DA.
[823] Article 3, 13, 14and 27 GDPR; 3,(g) and 31 Data Act.

subjects that are liable, such as the MDR[824]. This change is also required by the fact that, according to the proposed General Safety Product Regulation[825], online marketplaces could also be liable for the defects of the products they actually sell [826]. If we think that via several IoT objects for the home it is possible to access platforms and buy goods and services, then it is important that the updated PLD is also harmonised with the safety regulation, given the relationship of complementarity characterising them. Moreover, with reference to the notion of producer in Article 3 PLD, both the SDG and DCSD introduce the notions of trader and seller which will be involved in the supply chain of IoT objects for the home whenever non-contractual damages arise. It could be useful to add them to the list of possible "producers" in a future Article 3 PLD, as well as a representative of the producer (such as the importer) for non-EU companies which sell IoT products in the EU Digital Single Market. In this way, consumers might be able to recover the damage they endured from the subject with which they had the most contact. In many cases, the contact point could be the seller or the trader rather than the actual producer. Furthermore, in the new hypothetical Article 3 PLD, there should also be the mention of the data controller and data processor, which in many cases may correspond to the producer, and sometimes the trader or the seller of the connected object. This would be in order to better coordinate the documents directly or indirectly concerning home IoT objects.

3.1.3. Future Article 4 PLD

Article 4 PLD concerns the elements that the victim/plaintiff need to prove to receive compensation. Article 4 lists the damage[827], the defect[828] and the causal relationship between defect and damage as the elements the plaintiff must prove. This article is actually a bridge to Article 6 PLD on the defect and Article 9 on damage, as one cannot state that they have met the requirements of Article 4 without also successfully proving the elements specified in Article 6 and 9. However, more recently, Article 4 PLD has become important because it is a gateway for the CJEU to evaluate whether the systems to prove evidence in the MS are compliant with the directive. Contrary to what AG Geelhoed stated in his Opinion in *Commission v France I* [829], the directive does not have explicit competence for the harmonization of MS civil procedural law concerning the PLD. This did not stop it from doing so in *Sanofi Pasteur*[830]*.* In subsection 2.2 of this Chapter there was a detailed description of the reasoning of both AG Bobek and

[824] ELI response (2022),14.
[825] Arianne Sikken, " General product safety regulation: Council adopts its position," European Council website-press release, 20 July 2022, Accessed 31 January 2023, https://www.consilium.europa.eu/en/press/press-releases/2022/07/20/general-product-safety-regulation-council-adopts-its-position/.
[826] ELI response (2022),14.
[827] More infra at subparagraph 9 perspective PLD.
[828] More infra at subparagraph 6 perspective PLD.
[829] §§76-79: The EC had competence not only to regulate liability for defective products but also the procedures related to that, *Opinion of Advocate General Geelhoed Commission v France*.
[830] *Sanofi Pasteur,* C-621/15.

the CJEU which I will not repeat here. Suffice to say that the main principles that the courts must take into account to evaluate their national evidentiary law are the principles of effectiveness and equivalence. These principles must be exercised by national judges by taking into account their legal habits in interpretation, and must not lead to unbalanced and extreme results such as ignoring many elements pointing to the proof of a fact, or an omission. *Vice versa*, national judges' legal habits in interpretation must not be applied in order to reach a result in which inconclusive facts are taken into consideration to demonstrate something. What the CJEU still asks, and this is a demonstration of the fact that the PLD is still applied as a regulatory instrument and not a consumer protection one (despite the appearances), is that national judges assess whether the national procedural implementation rules are neutral in relation to the burden of proof of Article 4 PLD. In addition to this, national procedural implementation rules must not harm the effectiveness of the system[831]. The principle of neutrality of national rules on the Article 4 system could be a problematic tricky issue. As in the cases connected to alleged side-effects of vaccines, even technologies can create damages that are difficult for the users- consumers to prove.

In a near future, a national procedural rule could use the principle of "logging by design" described by the Expert Group on the Liability of AI and new technologies[832]. Would it be considered neutral in the overall balance of the directive? Logging by design is a principle which implies that the creator of an algorithm (an operator, in the language of the report[833]) or the manufacturer of a new technological object must design their connected products in such a way that there could be logs of the algorithm or machine activity, in compliance with trade secrets and IP law[834]. If there is no possibility of logging data concerning the activity, then the plaintiff could use legal, rebuttable presumptions against the operator/IoT producer which could concern a) causation, b) fault and/or c) the existence of a defect[835]. In order for these suggestions to be "neutral" on the effectiveness of the PLD, the new article 4 should make a reference to national procedural laws by taking inspiration from the contents of the *Sanofi Pasteur* judgment and opinion. Furthermore, with regard to new technologies, the future Article 4 should mention logging by design as an idea that the national legislator could use. In any case, if logging by design was included in a final text, it would be an exceptional matter, as insurances group already made it clear that they do not agree with this suggestion[836] and producers would most probably oppose this measure that would see their premium and research and development costs rise.

3.1.4. Future Article 6 PLD

[831] §33, *Sanofi Aventis* C-621/15.
[832] See Chapter III, Section 3.
[833] In the report lexicon, it is the person who is charged with the front-end and back-end operations and that corresponds in general to what the data processor is in data protection. See in Chapter III.
[834] Expert Group report [20]-[21].
[835] Expert group report, [22]-[24].
[836] Insurance Europe report (2021), 6.

Surprisingly, Article 6 PLD on the concept of defectiveness has only been questioned once before the CJEU. This happened in joint cases known as *Bostonmedezintechnik*[837]. It was in an important judgment as it followed AG Bot's opinion that defectiveness must also be considered *in abstracto*, especially with high-risk medical devices such as pacemakers and defibrillators[838].

Despite all that, I believe that Article 6 PLD as it is currently written may become the centre of many litigation processes, as it will be applied to consumer connected objects but also to more complex ones. For instance, it is likely to be applied to damages caused by connected medical devices[839] and also to consumer IoT objects with mixed health and consumer functions, such as wearables such as smart-watches or future appliances for semi-autonomous elderly homes.

This is motivated by the real possibility that users-consumers' perceptions of safety are likely to change, especially as our homes are becoming connected, as extensively explained in Chapter IV, subsections 1.4 and 1.5. Safety in a connected environment does not only mean physical integrity, but also trust that said environment will not also harm us in a more subtle, psychological way[840]. The twin directives SDG and DCDS could be a relevant source of inspiration to make the PLD more suited to new home technologies as they deal with problems of conformity of connected goods, digital services and digital content. Moreover, the SDG and DCDS also depend on lack of safety as one of the features creating a conformity defect, which is imputable either to the trader or the seller.

Preliminarily, we must remember that Article 6 PLD is built on the consumer expectation test. That is why Article 6 PLD defines safety as the one thing that a person can legitimately expect. The consumer expectation test is not likely to be substituted by the actual criteria of the risk-utility test, which is now the dominant rule for assessing a defect in the US and which is founded on the Third Restatement of Torts (see Chapter VI). One of the reasons why it would not be easy to substitute the consumer expectation test is also because it has been copied and amended in other parts of EU private law (both consumer and contract law). For instance, it appears that a kind of consumer expectation test is also encoded within the same Article 7 SDG and Article 8 DCDS, as the definition of conformity is also modelled also on a consumer expectation test: Article 7 (a) SDG expressly mentions in the objective requirements for conformity that the goods shall "[…] *be fit for the purposes for which goods of the same type would* ***normally***[841] *be used, taking into account, where applicable, any existing Union and national law, technical standards or, in the absence of such technical standards*, *applicable sector-specific industry codes of conduct*". Further, in article 6(a) SDG concerning the objective criteria for conformity, the object must have the "[…] *functionality, compatibility, interoperability and other features, as required by the sales contract*". In the future Article 6 PLD, there will probably be

[837] *Bostonmedezintechnik* C-503/13, C-504/14.
[838] §§29-31, *Opinion of Advocate General Bot Bostonmedezintechnik*.
[839] See Article 10(16) MDR.
[840] More on this in Chapter IV on the new conception of connected home and liability as trust.
[841] Emphasis added.

a reference to technical standards, codes of conduct or mechanisms of certification which might be part of EU harmonised standards in the New PLD, as they will be part of the factors that make a new technology trustworthy, hence, safe in the consumers' expectations.

It is also likely that an obligation to provide the necessary security updates in the SDG and DSDC[842] might also be added to a possible list of behaviours that make the consumer expect a normal level of safety. Lastly, the connected objects are always, directly or indirectly, under the control of the producer, which monitors the good functioning of the object. As a consequence, the expression "put into circulation" does not really make sense in the way that it used to and might also lead to the cancellation of the cause of justification of Article 7(b) concerning the existence of the defect at the moment of it being put on the market[843].

3.1.5. Future Article 7 PLD

Article 7 PLD has been one of the most contested before the CJEU, and I believe the exemptions for producers' liability will still be debated even with new technologies such as the IoT for the home. This is due to the fact that they are the main legal instrument that the producer can use against the plaintiff's claims if the plaintiff has managed to give full proof of the elements listed in Article 4 PLD (damage, event and causal link). However, if the PLD continues to be a mainly regulatory-harmonising instrument, producers also deserve exemptions which take technological advancements into consideration.

While the cases analysed in the two case-studies concerned Article 7(a)/(c)/ (d)and (e) of the PLD, the major arguments against the way in which the IoT works may only concern Article 7(a) and (b). These exceptions to the producers' liability respectively concern the fact that the producer did not put the product into circulation[844] and that the defect did not exist when the product was put into circulation[845]. These two exceptions will not be easy to apply to connected objects such as the domestic IoT. This is due to the fact that connected objects are always, directly or indirectly, under the control of the producer, which monitors the good functioning of the object. Hence, the expression "[to] *put into circulation*" does not really make sense in the way that it used to and might also lead to the cancellation of the cause of justification of Article 7(b) concerning the existence of the defect at the moment of it being put on the market[846].

With reference to the first exception, every item of a technological object now has an identifier (via bar-codes or RFID tags), hence it is virtually impossible not to know who marketed/produced the product or even the single physical part

[842] Articles 7(3)(a) SDG and 8(2),(a),(b).
[843] Joasia Luzak, "A broken notion: Impact of modern technologies on product liability," *European Journal of Risk Regulation* 11,3(2020):631; ELI response to public consultation (2022):16.
[844] Article 7(a) PLD.
[845] Article 7(b) PLD.
[846] Joasia Luzak, "A broken notion: Impact of modern technologies on product liability," *European Journal of Risk Regulation* 11,3(2020):631; ELI response to public consultation (2022):16.

of it and whether the defect might have already been present at the moment it was marketed[847]. The true matter is to ascertain what "being put into the market" means with new technologies as both Article 7(a) and (b) make reference to it.

If we apply the teleological interpretation of AG Geelhoed in *O'Byrne,* what should be used is a flexible notion of the term "control". He made an elaborate analysis of the diverse organisational models within multinational companies. In this case the AG took into consideration the notion of "group at large" and, in that case, the moment when the product was put into circulation was when it exited the sphere of control of the group[848]. Moreover, one could argue that the notion of "sphere of control", created by AG Geelhoed in *O'Byrne,* as the moment when the product is placed on the market, could be the antecedent legal model on which the GDPR's figures of the controller and processors are based, as well as the basis of the vendor's liability both in the SDG and the DSDC. These reflections could be also applied to Article 11 PLD on the duration of the producer's liability, as it also depends on the moment when the product is put into circulation.

In the context of the IoT supply chain, the application of *de facto* control or sphere of control could be applied to the "big multinational group" model - one of the two models of IoT production described in Chapter IV - which summarise the supply and value chain of the IoT. However, this rationale could also be used in the second model (the one in which there are several subjects involved but the producer may not have *de facto* control over many of the parts or the functioning software). In this way, by focusing on who has the *de facto* control, it is possible to identify the producer more easily and to evaluate the starting point of the producer's liability more accurately. It could be argued that, in the moment in which the IoT object is bought by the consumer, the sphere of control of the producer-manufacturer ends and a new duty (e.g., to follow-up, to provide updates) ensues. In this way the producer would not be considered forever liable.

Article 7 PLD also hints at accountability and responsibility in a moral sense: already in *Veedfald,* it was established that the producer could not say that it did not make the product once it was discovered at a later moment that it was defective. That was at the beginning of the case law concerning the PLD[849]. The considerations made for Article 7(a) and (b) PLD also apply to the logic of Article 7(c) PLD, which involves the proof that the product was not made by the producer. Article 7 letters, (d) and (f) are rather straightforward and *a priori* should not cause any clash with domestic IoT product. Article 7(d) concerns the exception of whenever the defect is caused by compliance with mandatory

[847] Joasia Luzak, "A broken notion: Impact of modern technologies on product liability," *European Journal of Risk Regulation* 11,3(2020):631.
[848] In that particular case, it was also the matter to establish which company had put the allegedly defective vaccine into circulation in order to determine whether the plaintiff was time-barred. See §§ 31-51 *O'Byrne v. Sanofi* C-127/04.
[849] §23 "Opinion of Advocate General Ruiz-Jarabo Colomer, Henning Veedfald v. Århus Amstkommune C-203/99," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A61999CC0203&qid=1484153976108 .

regulations. This is an exception and, like all the exceptions in the internal market, requires a strict interpretation[850].

The most problematic (even in pre-IoT times) of these exceptions is the one regarding risk development, namely Article 7(e) PLD. Its history was not an easy one: some countries insisted on having it in the directive to try to balance the producers' reasons with the consumers'. As it was quite a divisive topic, because the views concerning consumer protection differed across the MS, the directive allowed flexibility for the states in transposing it[851]. It is interesting that the first judgment before the CJEU concerning the PLD concerned the doubts on how the UK government had transposed this exception[852]. The Commission argued, unsuccessfully, that the former MS had applied a subjective interpretation of the clause. The British transposition allowed producers to be exempted from liability every time they demonstrated that there was no particular risk for the product to be unsafe, basing this belief on their personal state of knowledge. The Court followed AG Tesauro in considering that the clause must be interpreted objectively[853] and that it was important to take not only the technical standards or the learned opinion of the majority but *"[…] the most advanced level of research that has been carried-out at a given time."*[854] The other judgment concerning the implementation of this exception was the one from France, which altered the text to favour consumers, in line with its tradition[855]. Despite the application field of this exception seeming clear in theory and it being likely that it will stay in a possible updated PLD as it is in the producers' and manufacturers' interest, the reasoning of AG Tesauro is difficult to apply in practice with home IoT objects.

Is it really possible to discover the most advanced level of research as technology evolves at an increasingly faster pace? This would mean that companies should devote a consistent part of their budget to research and development in order to remain constantly updated and should not only take conclusions from their results but also from the "*most advanced level of research* which has been carried out at a given time"[856] which is difficult to define objectively.

3.1.6. Future Article 9 PLD

[850] §15 Judgment Veedfald, C-203/99.
[851] Luxembourg and Finland chose to include the risk development option. Spain decided to exclude it for certain high-risk products; France excluded the produits de santé from the human body. Germany at that time excluded pharmaceutical products as it had already regulated them in a special law of 1976. Duncan Fairgrieve et al. "Product Liability Directive," in *European Product Liability: An Analysis of the State of the Art in the Era of New Technologies*, Piotr Machnikowski (Antwerp, Cambridge, Portland: Intersentia 2016),29.
[852] *Commission v UK* C-300/95.
[853] §27, *Opinion of Advocate General Tesauro Commission v UK.*
[854] § 21, *Opinion of Advocate General Tesauro Commission v UK.*
[855] §47 Commission v. France C-52/00.
[856] [856] § 21, *Opinion of Advocate General Tesauro Commission v UK.*

Article 9 PLD concerns damage and even in pre-IoT times it was one of the mostly discussed articles before the court. It was suggested that the reason for this uncertainty in this article's interpretation might also rely on its "*rather confusing draft*"[857]. As already specified at the beginning of this chapter, Article 9 PLD concerns both physical injury (including death) damages but also damage or destruction of private property for no less than 500 euros and only if the object damaged was "[…] *ordinarily intended for private use or consumption, and* […] *was used by the injured person mainly for his own private use or consumption*"[858]. For these two causes of damage, each MS must provide full compensation, but, as Article 4 case law previously established, the MS must determine the contents of these rights without impairing the effectiveness of the Directive[859]. Financial loss is also recoverable if it is consequential to personal injury or loss of property, if national law allows, but the PLD does not admit pure economic loss, as instead it may appear to do from reading the *Veedfald* judgment[860]. With the *Dalkia Somer* judgment, there is also the exclusion of damage to property not intended for private use or consumption[861]. Moreover, both in *Commission v France I* and in *Commission v Greece* the threshold was criticised by the MS because it would have deprived consumers of access to justice, but these opinions were rejected as it was still possible for citizens to sue the producers according to national rules.

The fact that Article 9 PLD, together with Article 7 PLD, has been brought before the CJEU most frequently after Articles 3 and 13 PLD makes it likely that it will be necessary to amend it also to accommodate new instances concerning technology. Academics and groups of interests have already started giving suggestions on the matter. For instance, both the ELI's response and the Insurance Europe report advocate that pure economic loss and moral damage continue to be excluded from the update of the PLD[862]. However, the response of the ELI states that there must be compensation for the pecuniary consequences which derive "[…] *from pain and suffering triggered by bodily injury, and not to stand-alone immaterial harm, such as purely emotional distress*."[863]

At this point, it is interesting to investigate which possibly "new" sources of damage the PLD could grant compensation for. This can be done by analysing *a contrario* the instances of European insurance groups.

---

[857] Duncan Fairgrieve et al, "Product Liability Directive," in *European Product Liability: An Analysis of the State of the Art in the Era of New Technologies*, Piotr Machnikowski (Antwerp, Cambridge, Portland: Intersentia 2016),32.
[858] Article 9(b)(i)(ii)PLD.
[859] Duncan Fairgrieve et al, "Product Liability Directive," in *European Product Liability: An Analysis of the State of the Art in the Era of New Technologies*, Piotr Machnikowski (Antwerp, Cambridge, Portland: Intersentia 2016), 32.
[860] Duncan Fairgrieve et al., "Product Liability Directive," in *European Product Liability: An Analysis of the State of the Art in the Era of New Technologies*, Piotr Machnikowski (Antwerp, Cambridge, Portland: Intersentia 2016),32- 33.
[861] Duncan Fairgrieve et al., "Product Liability Directive," in *European Product Liability: An Analysis of the State of the Art in the Era of New Technologies*, Piotr Machnikowski (Antwerp, Cambridge, Portland: Intersentia 2016), 33-34.
[862] ELI response (2022) 17.
[863] ELI response (2022) 17.

While insurers agree on the fact that producers could be held strictly liable for the failure to provide security updates, they strongly disagree on another series of issues arising from the use of connected objects such as the domestic IoT[864]. These are the possible contents of the directive that the group objects to:

1) *"The Directive should harmonise the right of consumers to claim compensation from producers who are not simultaneously data controllers or processors, for privacy or data protection infringements (e.g., a leak of personal data caused by a defect)*
2) *The Directive should harmonise the right of consumers to claim compensation for damage to, or destruction of, data (e.g., data being wiped from a hard drive even if there is no tangible damage)*
3) *The Directive should harmonise the right of consumers to claim compensation for psychological harm (e.g., abusive robot in a care setting, home-schooling robot)*
4) *Some products, whether digital or not, could also cause environmental damage. The Directive should allow consumers to claim compensation for environmental damage (e.g., caused by chemical products) coverage*
5) *Other kinds of damage*" [865]

It is understandable why environmental damage should be excluded, as it has a specific discipline, hence nothing more than a reference to the ELD should be included in the future PLD. This reference to the ELD will be important regardless, as European citizens have demonstrated that they are attentive to environmental themes and technology, hence liability should bear this in mind. Nevertheless, I am not sure that the other three options (1, 2, 3) should be left completely to the MS' initiative. Unlike the time when the PLD entered into effect, options 1 and 2 are not in a legal void: the GDPR and the Data Act now exist, which regulate similar phenomena to the ones the new PLD will have to deal with.

Unfortunately, the problem is that neither the GDPR nor the DA regulate liability directly, as it still is the competence of the state to create and implement remedies for the violation of both the DA and the GDPR. Moreover, the DA only concerns the rules on access to data and, in principle, how to draft fair data access contractual clauses and contracts. It is true that the DA contains Article 13 DA, concerning the invalidity of unfair contract, but then it is up to the MS to enforce it in their systems. Besides, the DA is still at a proposal phase: therefore, it may be some time before any hypothesis of contractual liability enforcement of the DA might present itself.

The GDPR includes Article 82 GDPR, which establishes the principle of full compensation for any violation of said legislative act. Article 82 GDPR also states that both material and immaterial damages must be compensated[866] and that the data subject can request compensation for damages from different controllers or processors and then the one that paid damages will be able to commence a recovery action against the others[867].

[864] All the following cases can be found in the already cited Insurance Europe report at page3.
[865] All the following cases can be found in the already cited Insurance Europe report at page3.
[866] Art 82(1) GDPR.
[867] Art 82(4),(5) GDPR.

The main problem with private enforcement of national data protection is that, depending on the different national legal traditions, there may be difficulties in interpreting the core part of Article 82 GDPR, which establishes full compensation for any (literal) violation of the GDPR, for both material and immaterial damage. Hence, private enforcement of Article 82 GDPR is simply not effective after four years, because it was partly conferred on the states, contrary to what Insurance Europe claims. In particular, immaterial damage is difficult to evaluate in countries such as Germany, where tort liability is governed by a strict rule, as seen in Chapter IV. That is why it is not surprising that in Germany there are already many cases about how to prove and the extent of immaterial damage[868]. On the contrary, in Italy, where there is quite a flexible extra-contractual liability clause, the Italian Court of Cassation took a firm stance in 2021, stating by means of an *Ordinanza* that it is not possible to claim compensation, even due to violation of GDPR, without proof of damage[869].

In the end, the Austrian Supreme Court conducted a preliminary reference procedure asking *i)* whether the plaintiff must always show that he has suffered damage or whether solely a breach of the GDPR is sufficient; ii) whether there are other principles besides the ones of effectiveness and equivalence iii) and whether there is a pre-condition to award the non-material damage on the basis that the GDPR violation must not just cause a mere annoyance [870]. The opinion of AG Sánchez-Bordona on this case was published last 6th October 2022[871]. In the AG's very long and articulated opinion in which he takes into account several ways to interpret Article 82 GDPR (such as a literal, a legislative-history-based, a contextual and a teleological interpretation[872]) and in which he explores the possibility that the GDPR entails a sort of punitive damage for its mere violation[873], the AG concludes that it is indeed needed that the data subject gives proof they have suffered damage[874].

While waiting for the CJEU judgment, and despite the Court of Cassation *Ordinanza,* scholars in Italy are still undecided about considering the violation of the GDPR as a *danno evento* (damage connected to an event), therefore always

[868] " GDPR Violations in Germany: Civil Damages Actions on the Rise," *Latham & Watkins Litigation & Trial and Data Privacy & Security Practices*, December 18, 2020, https://www.lw.com/admin/upload/SiteAttachments/Alert%202821v7.pdf.
[869] Ordinanza Cassazione n.16402/2021, Accessed 31 January 2023 https://i2.res.24o.it/pdf2010/Editrice/ILSOLE24ORE/QUOTIDIANI_VERTICALI/Online/_Oggetti_Embedded/Documenti/2021/06/11/16402.pdf .
[870] GDPR HUB,OGH-6Ob35/21 x, Accessed 31 January 2023, https://gdprhub.eu/index.php?title=OGH_-_6Ob56/21k_(request_for_preliminary_ruling_under_Article_267_TFEU). Request for a preliminary ruling from the Oberster Gerichtshof (Austria) lodged on 12 May 2021 – UI v Österreichische Post AG (Case C-300/21), Accessed 31 January 2023, https://curia.europa.eu/juris/document/document.jsf?text=&docid=244568&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=668819.
[871] "Opinion of Advocate General Campos Sánchez-Bordona delivered on 6 October 2022," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1675182921469&uri=CELEX%3A62021CC0300 . Hereinafter, Opinion C-300/21.
[872] Opinion C-300/21, §§ 35 -82.
[873] Opinion C-300/21, §§ 35-82.
[874] Opinion C-300/21, §117.

subject to compensation. This interpretation would be compliant with the literal interpretation of Article 82 GDPR[875]. Some other scholars, instead, claim that GDPR damage is a *danno conseguenza* (damage connected to a consequence), which must actually be proved by the plaintiff, especially the damage aspect. This seems to be the majority view, as it is also the one held by the *Ordinanza* of the Italian Court of Cassation and other scholars[876].

In Italy, the uncertainty connected to compensation for immaterial damage caused by a GDPR violation will remain until the CJEU judgment even though the Opinion of AG Sánchez-Bordona might indicate that the CJEU will have a similar view on the topic. Moreover, a recent *revirement* of the Italian Court of Cassation in 2018[877] once again tried to provide indications (this time through a ten-point bullet list) regarding the main division between pecuniary and non-pecuniary damage, an issue that has also been debated for a long time and that has prompted other important judgments[878] and that will certainly be used to evaluate immaterial damage caused by data processing also by the home IoT. The non-pecuniary damage category comprehends moral damage, and in general, can be equalised to the non-material damage in Article 82 GDPR[879]. Non pecuniary damage is linked to the violation of personal and economic rights and interests that are protected by the Constitution[880], hence, privacy and data protection could be protected thanks to the use of Article 117 of the Italian Constitution, which makes it possible to apply international and EU law in the Italian legal system. As far as the method to calculate damages is concerned, the Italian Court of Cassation made it explicit that the system in use prior to its *revirement* in 2018, based on the tables created by the judges in Milan, was no longer convenient. Instead, the method of the *sistema a punto variabile* was considered more suitable for the new theoretical approach to liability.[881].

Simply put, the effective private enforcement of GDPR liability is currently non-existent, with many existing differences among countries. Moreover, it is also fair to say that at the moment there is no effective enforcement model for damages created by data processing. Hence, since it is not yet possible to count

---

[875] Emilio Tosi, *Responsabilità Civile per Illecito Trattamento dei Dati Personali e Danno non patrimoniale. Oggettivazione del Rischio e Riemersione del Danno Morale con Funzione Deterrente e Sanzionatoria* (Milano: Giuffrè Francis Lefebre,2019). Hereinafter Emilio Tosi *Responsabilità Civile* (2019); Rossana Ducato, "LA LESIONE DELLA PRIVACY DI FRONTE ALLA "SOGLIA DI RISARCIBILITÀ": LA NUOVA MAGINOT DEL DANNO NON PATRIMONIALE?," *Trento Law and Technology Research Group* (2016), 125-148.

[876] To have a full overview of the Italian legal scholars' opinion on these issues, see Shaira Thobani, "Il Danno Non Patrimoniale Da Trattamento Illecito dei Dati Personali (Estratto)," *Diritto dell'Informazione e dell'Informatica* (2017): 452-455.

[877] Italian Court of Cassation, Third Section, n.7513/18, (President Judge: G. Travaglino, reporting judge: M. Rossetti), Altalex, Accessed 31 January 2023, https://www.altalex.com/massimario/cassazione-civile/2018/7513/risarcimento-del-danno-patrimoniale-e-non-patrimoniale-danni-morali-congiunta-attribuzione; Emilio Tosi, *Responsabilità Civile per Illecito Trattamento dei Dati Personali e Danno non patrimoniale. Oggettivazione del Rischio e Riemersione del Danno Morale con Funzione Deterrente e Sanzionatoria* (Milano: Giuffrè Francis Lefebre,2019), 212-216. Hereinafter Emilio Tosi *Responsabilità Civile* (2019).

[878] In particular, Court of Cassation 31 May 2003 n. 8827, Court of Cassation 31 May 2003 n. 8828 and Court of Cassation Plenary Session (Sessioni Unite) 11 November 2008 n. 26972, n.26973, n. 26974 and n. 26975.

[879] Emilio Tosi, *Responsabilità Civile* (2019),217.

[880] Emilio Tosi, *Responsabilità Civile* (2019),212-216.

[881] Emilio Tosi, *Responsabilità Civile* (2019),212-216.

on GDPR for private enforcement, it is not possible to count on national enforcement strategies right now with a CJEU case pending, contrary to what the Insurance Europe group stated in its report. Furthermore, despite data's considerable economic worth, it is also not clear how MS will enforce the contracts for access to data. The Data Act establishes dispute settlement mechanisms but relies on MS for contractual rules on liability. Also, while it might be less complex to qualify pecuniary loss compared to immaterial damage from a data breach, the quantification of pecuniary loss connected to lost data is also not a simple matter as there are no standardised methods of quantification. Instead, everything is left to the common sense of the judiciary.

If the end objective is the creation of a Digital Single Market, we should take this occasion to regulate the new PLD in the best way possible, in order to further harmonise effective remedies for EU citizens. One idea could be to add a mention in the future Article 9 that damage to the physical and psychological integrity of an individual can also be the consequence of defective data processing, which may or may not involve personal data. In this way, whenever there is a CJEU judgment on the matter, it will be easier to coordinate the two regimes.

Moreover, as the English case *Lloyd v. Google*[882] showed recently, it could also be possible that several people suffer from the same kinds of immaterial damages (for instance data leaks which cause damage to property and create bodily injuries) and that collective actions may sometimes prove unsuccessful compared to individual ones. However, the cost of maintaining these legal battles individually prevents people from going to court, especially if it is difficult to prove damages (such as technology-induced moral or psychological damages) and even if there is evident damage, such as in the PIP saga, the EU tools for collective redress were not always effective. For this reason, a paragraph should be added that makes reference to Annex I (i) of the directive on representative actions[883] which already contemplate the possibility of bringing collective actions for matters involving the PLD in Article 1(1) of its Annex I.

3.1.7. Future Article 11 PLD

During the development of this chapter, articles of the PLD have often been combined together in the same judgment. Within a judgment, one or two articles read as complementary to each other, or which are different but intrinsically connected (for instance more procedural and substantial articles). This was true for Article 13 PLD[884] and this is also true for Article 11 PLD, which

[882] "Lloyd (Respondent) v Google LLC (Appellant), UKSC 2019/0213," The Supreme Court (official website), Accessed 31 January 2023, https://www.supremecourt.uk/cases/docs/uksc-2019-0213-judgment.pdf . Hereinafter *Lloyd v Google*.
[883] "Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC," EUR-Lex, Accessed 31 January 2023 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2020.409.01.0001.01.ENG .
[884] More on this in the next subparagraph, Article 13 perspective PLD.

concerns the number of years for which the producer could be held liable, which in this case is ten years.

The issues connected to the producers' liability time limit have overlapped with problems connected to the qualification of producer in Articles 3 and 7 PLD. In *O'Byrne* and *Aventis Pasteur* the complex structure of the internal organisation of pharmaceutical companies producing vaccines caused two people to sue the wrong subject and result in being time-barred, as in *Aventis Pasteur*. I think that developments connected to the identity of the producers described in *supra*[885] will continue even under the new PLD. In Chapter IV, the complications of the IoT supply and value chains were considered as one of the most problematic aspects for the allocation of liability, not just when there was solely an international producer (model 1), but especially when different actors (producers-manufacturers, cloud services providers, platforms, internet services providers) are involved (model 2). This is because even under a relationship of delegation (from the producer to the subject tasked with data processing, such a sub-contractor, for instance), the formal producer might not have a meaningful control over the process, especially when serious damage ensues. However, if we combine the recent interpretation of Article 3(1) in *Fennia v. Philips*, the rules on national evidentiary procedures of Article 4 PLD in *Sanofi Pasteur* and the rules of *O'Byrne* and *Aventis*, there may not even be the need to amend the number of years of liability and maintain the rule of Article 11 just as it is.

3.1.8. Future Article 13 PLD

In sub-section 2.2, the qualitative analysis of the judgments led me to interpret them as all connected, directly and indirectly, to the distribution of competences between the EU and the different MS, which in the PLD is an issue that is recalled indirectly in Article 13 PLD. I explored the evolution of the contrasts and dialogue between the MS and the national courts with the AGs and the CJEU and I found that, while in an initial period Article 13 PLD was tackled directly, alone or in combination with other articles (especially Article 3 PLD), in a subsequent period the judgments concerning Article 13 PLD was not directly challenged. Nevertheless, for this second period there are two kinds of judgment concerning Article 13 PLD. The first group of judgments is not particularly interesting because the CJEU applied quite regularly the previous jurisprudence on Article 13 PLD. On the contrary, the second group of judgments is characterised by cases that used the PLD and the notion of its compatibility with Article 13 PLD to also harmonise national procedural rules concerning evidence. While, at a first look, this last series of judgments seemed more open to the implementation ideas from national courts, the doctrine of maximum harmonization and the respect of the principles of effectiveness and equivalence

[885] Subsection Article 3 perspective PLD.

in order to not undermine the application of the PLD always lingered in the sub-text of the opinions and judgments, even when not explicitly referred to[886].

In the future, it is unlikely that the legal basis will change or that a the Treaty would be amended before a new proposal for an updated PLD. Hence, with all probability, the legal basis will remain the harmonization clause of Article 114 TFEU, used more or less correctly for digital issues, even if Article 114 TFEU is broader in application than its antecedents.

What does this mean for the future of Article 13 PLD? The main points of the judgments must be analysed to determine whether they could be applied to new technologies or not. The first point is the maximum harmonization clause: it should be made explicit either in Article 13 or in a new dedicated article. There are mainly two reasons for this. The first is the respect of all the previous case law on the matter. The second reason is that the two main contractual liability instruments for the IoT (SDG and DCDS) are also maximum harmonization directives according to their respective Article 4[887]. The second point concerns the possibility of inserting a recital and a paragraph in Article 13 PLD, which concern the rules of the principle of effectiveness and equivalence as it concerns implementation of the PLD, which could be applied to national procedural rules. In this way, the MS would be bound to create tools that, even though formally different, would allow progressive harmonization of the effects of the directive's consumer remedies. Finally, the part concerning acquired rights should be updated with the core of the judgment of *Novo Nordisk Pharma*, which made the passage more explicit.

New problems may arise concerning concurring systems of liability for the new PLD. However, these days, the concurring liability regimes are more likely to originate from the transposition of EU legislative acts into EU law. For example, the producer might also be a seller for a pre-installed app on the IoT consumer device that did not provide security updates as frequently as it should have. Let us imagine that because of that fault of the seller and the contract tying them to the supplier of the service (the pre-installed app), damage to property and physical damage ensued. This situation involves the SDG and also the PLD (even without modifications), as the provision of security updates by the producer make the consumer have certain expectations regarding the safety they can expect from the product, but they should also be part of the contract between the seller and the consumer. Therefore, it is likely that the article should be modified in a way to accommodate the previously cited case law and also to allow the possibility for the cumulus of two kinds of liability actions: one based on the PLD and the other one on the SDG or DCDS, or even the GDPR, whenever the national procedural laws allow it as an option. Moreover, one has to take into consideration that PLD's field of application may even already be more extensive, even without a formal update. In fact, Article 10(16) MDR recalls the application of the PLD to medical devices. The MDR will also probably be applied to IoT with

[886] For more details on the judgments and opinions which led to these conclusions see sub-section 2.2 of this chapter.
[887] See Articles 4 of SDG and DCDS

healthcare functions, hence, the PLD might end up in being applied to what the Expert Group on liability might consider high-risk devices and not only low-risk devices such as IoT for the home. However, it is important to notice that Article 10(16) MDR also mentions a special rule for medical devices: the rule is that the PLD rules will apply if the medical device causes damage, but more protective national liability frameworks may be applied, thus applying the rule of the *Schmitt* judgment[888].

4. Preliminary conclusions

In a certain way, the PLD can be described, if not as a success story because of the relatively low number of cases brought before the CJEU, at least as one part of the *EU Consumer Acquis* law that has been consolidated for the longest period of time without major amendments. It has been argued that this was substantially due to three factors. The first reason is the general higher quality and safety for consumer objects that is required by the EU single market in general than in other countries[889]. The second reason is the cap of 500 euros in order to apply the directive for property damage and, as third reason, the short time for the claimant to act when the damage happens[890]. One might disagree with the argument of higher general safety: after all, several judgments of the database concerned vaccines and medical devices of various types which showed the shortcomings of the interaction between the PLD and supposedly more protective regimes such as the MDD now MDR (New Legislative Framework).

Despite all the critical remarks made by the scholars, MS and national judges, the PLD is here to stay and to adapt to new technologies. This includes the IoT and the next step, the IoE, which will make the problems highlighted in this section even more evident, given the higher level of interconnectedness with human beings than the IoT. The best that can be done is to ensure that past mistakes and legal ambivalences have been learned and to try to create a new framework that already ensures a meaningful connection to the future *Digital Consumer Policy Acquis*. That is what I have tried to do in the third section of this Chapter.

To make this analysis more complete, in the next Chapter I will analyse the peculiarities of the US system of product liability and how that system is responding to the IoT technologies for the home.

---

[888] See in Chapter II, sub-section 1.3.2 and Chapter VI, subsection 2.3.2.2.
[889] Piotr Machinkowski, "Conclusions," In *European Product Liability: An Analysis of the State of the Art in the Era of New Technologies*, Piotr Machnikowski (Antwerp-Cambridge-Portland: Intersentia, 2016), 669-705.
[890] Piotr Machinkowski, "Conclusions," In *European Product Liability: An Analysis of the State of the Art in the Era of New Technologies*, Piotr Machnikowski (Antwerp-Cambridge-Portland: Intersentia, 2016), 669-705.

Chapter VI: IoE home devices in the US. Theory and cases

Chapter VI: IoE home devices in the US. Theory and cases 191
1. Introduction 191
2. The US model: past and current trends with new technologies 192
2.1. A concise evolution of the US products liability theories 192
2.1.1. A certain kind of negligence: probability considerations and the Learned Hand formula 194
2.1.2. The "attack" on privity: from the implied merchantability warranty to the Uniform Commercial Code 195
2.1.3. 1963: The strict liability doctrine and its influence on the Restatement Second of Torts 199
2.1.4. New defects under the Restatement Third of Torts, and products liability until today. 201
2.2. US priorities in technology regulation: platforms, AI and the IoT 204
2.3. The home IoT and the American legal scholarship 212
3. Case law on consumer IoT devices in the US 216
3.1. Security devices for the home 218
3.1.1. FTC cases 218
I. TRENDnet 220
II. Vizio 221
III. D-Link 222
IV. Tapplock 224
V. Comparison with EU law 226
3.1.2. Judicial case: Onity 226
I. Comparison with EU law 231
3.2. Toys and children's devices 231
3.2.1. VTech Data Breach Litigation 232
3.2.2. Archer-Hayes v. Toytalk, INC. 235
3.2.3. A comparison between Archer-Hays and V-Tech and EU law 236
3.3. Medical devices and IoT with medical functions 237
3.3.1. The Therac-25 Case. An ante litteram IoT case 238
3.3.2. The St Jude Medical LLC cases 239
I. American preemption and the St. Jude Medical LLC cases: Freed III, Mellott, Guinn and Ross 239
II. Comparison with EU law: which liability for IoT with medical and consumer functions? 246
3.4. Connected cars 248
3.4.1. Comparison with EU law 253
4. Some preliminary conclusions 255

1. Introduction

This chapter has one main function: to compare and contrast the EU system of product liability with another legal model, the US one. There are several reasons to choose the US as a term of comparison. Firstly, IoT technology was

created in the US, and it is at the basis of the future IoE. Secondly, even if the US legal background concurred in making this technology thrive, there are no studies in Europe that compare and contrast the IoT regulatory models of the US and the EU at the moment of writing. Thirdly, in the US there have been already a considerable number of cases involving IoT objects that can be referred to as domestic IoT objects. This could be a source of great insight concerning the types of damages to expect also in an EU context and, furthermore, despite the legal system differences, it could also be insightful regarding the kind of legal actions to be expected. The first part of this chapter (2) will concern the product liability rules and theories in the US but also a brief summary of the main differences with the EU approach. This is in order to give an EU reader the basic tools to interpret the judgments (2.1). There will then be an analysis about which kind of regulation (if any) is going to be applicable for the domestic IoT and whether it will influence the remedies that are already available in the US (2.2). The last part of this second section will be devoted to an analysis of how American legal scholars consider IoT technology (2.3). Finally, the second part of the chapter will contain comments of cases concerning IoT devices in the US (3). For each of the cases there will be a description of facts, the main legal questions and the reply of the court and, finally, a speculative analysis about the outcome and the reasoning of a fictional judgment if those particular cases had to be decided by the CJEU. Finally, there will be some preliminary conclusions (4). As a preliminary remark, I will use the expression "products liability" instead of product liability as the former is the most used way to refer to this branch of law, whereas the latter is more commonly used throughout the EU.

2. The US model: past and current trends with new technologies

The US model of products liability is a unitary label which makes reference to several legal theories: it ranges from tort theories, including negligence and strict liability, and extends also to contractual warranties[891]. It covers all the US constitutional levels, from federal, to national and passing through the evaluations of legal scholarships through restatements. It is useful to give a concise overview of the evolution of US products liability theories (2.1) before analysing the type of approach to technology regulation that is taking place in the US (2.2).

2.1. A concise evolution of the US products liability theories

Product liability in the US is a complex and still developing branch of private law which has partly also influenced the drafting of the original PLD. Despite the 51-state composition and the Common Law regime (which relies more on the courts' activity to create and/or find substantive rules,) the products liability rules tend to be relatively uniform across the country[892]. One of the most

[891] In the US, the label product liability is not common as it has a European origin and application. Conversely the expression 'products liability' is more familiar to US scholars and generic audience, hence in this chapter I will use products liability instead of product liability when making reference to the US theories and cases connected to damages caused by products.

[892] Michael Green and Jonathan Cardi, "Product Liability in the United States of America," in *European Product Liability: An Analysis of the State of the Art in the Era of New Technologies*, Piotr Machnikowski (Cambridge, Portland Antwerp: Intersentia, 2016) 576.

remarkable differences between the US and the European (*lato sensu*) models is that in the US there have always been considerably more products liability cases, ranging from defective production standards[893] to the most common and trivial accidents (such as Coca Cola glass bottles exploding[894]) but also involving serious cases such as blood contaminations or dangerous side effects of pharmaceutical products.

Before discussing how technology is affecting the rules on US products liability, it is essential to summarise the development of US products liability by bearing in mind not only the landmark judgments of federal and national jurisdictions, but also the development and change brought on by the Uniform Commercial Code and the Restatements Second[895] and Third of Torts. The relationships and ties between these different legal sources can provide a better understanding of how legal culture changes as well as society and public policy[896], and some insights on proposed legislative/regulatory outcomes in the domestic IoT field.

In addition, it is important to remember that, while EU product liability could be loosely assimilated to strict liability, this is not the case in the US. To summarise, one could say that, at the start, products liability theories in the US were addressed from two opposite point of view. The first one was also more in line with the tradition of English Common Law and involved the tort of negligence. The second one, closer to the French theory of the sale, involved an express or implied merchantability warrantee. The way in which they developed is described in the following subparagraphs[897]. However, the reader should bear in mind the fact that these theories developed almost at the same time. Even before the emergence of industrial machines or mass-produced objects that could hurt people, the *fil rouge* of the cases was always the same: a third party - who suffered damages - asked for damages from a party with whom they had no contractual relationship. However, most of the time, the plaintiff had an implied relationship with the alleged defendant(s), usually based on a position of control which they held. This control concerned a person, an object, an animal or a situation that had caused an injury or loss to the plaintiff. Products liability thus evolved to react to the unfairness towards a plaintiff due to initial lack of adequate legal remedies. While the relationship of actual control between manufacturer and object is never mentioned explicitly in the judgments that will be commented on, the unfairness of the plaintiffs' situation, who were without explicit legal remedies for a long period, is a theme that emerges frequently in almost all the judgments analysed.

---

[893] Paul Verbruggen, "Tort Liability for Standards Development in the United States and European Union," in *The Cambridge Handbook of Technical Standardization Law*, Jorge Contreras, (Cambridge: Cambridge University Press, 2019), 75.

[894] Such as in the case *Escola v Coca Cola*, Supreme Court of California, July 5, 1944.

[895] American Law Institute, *Restatement of the Law Second Torts 2D, Volume 2* (Saint Paul, Minnesota: American Law Institute Publishers,1965), §§281-503.

[896] Indeed, public policy was used by judges both to recognise compensation claims to plaintiffs but also to reject them. Regarding the first case, one example is *Henningsen v Bloomfield Motors Inc,* Supreme Court of New Jersey, May 6, 1960, which introduced liability without the limitation of privity beyond food and to defective products in general (14-15).

[897] These two theories were firstly introduced in Chapter IV separately and will be better described in the later sections with a specific reference with the US products liability development history.

2.1.1. A certain kind of negligence: probability considerations and the Learned Hand formula

Originally, cases concerning the liability of products were considered to belong to the part of tort law entitled negligence. Hence, the plaintiff had to demonstrate the elements that are required to establish the tort of negligence:

1) an actual *duty of care*, specified by a law or statute[898];
2) the defendant's *breach* of duty (generally the courts consider the breach as a founding element of negligence together with the duty of care)[899]
3) a causal connection, called *causation*, between the fact and the defendant's conduct[900] and
4) the resulting damage or actual loss[901].

One might think that these four elements are all easily distinguishable from each other. However, the truth is that their significance is relative to the contents of all the others[902], and this, I argue, is going to be even more evident with new technologies, but let us start by examining the relevant law using a chronological approach.

Throughout the second industrial revolution, until the beginning of the mass-consumer society, it was becoming increasingly difficult for plaintiffs to demonstrate the existence of the above-cited elements, especially the presence of a duty of care. American judges, like many of their European colleagues, proved to be sensitive to societal changes and started a process through which traditional negligence rules became more flexible. The first seminal case in this sense is *MacPherson v. Buick*[903]. This judgment established that the manufacturer had a greater duty of care towards the consumer than previously established: in this specific case, the duty encompassed the obligation for the defendant to inspect the car parts that were not made by the defendant itself, but by another party, with whom the consumer plaintiff had no contractual relationship[904]. Subsequently, in *Escola v. Coca Cola,* the Court stated that if the product did not work as promised (the bottle of Coca Cola exploded

[898] Victor E. Schwartz, Kathryn Kelly and David F. Partlett, *Prosser Wade and Schwartz's Torts. Tenth* edition (New York: Foundation Press,2000),130, hereinafter *Prosser Wade Schwartz.*
[899] Ibid. *Prosser Wade Schwartz*.
[900] This element needs both a factual connection but also a legal one, which is known as proximate causation. This will specifically be dealt with in section 2 of this chapter.
[901] Ibid. *Prosser Wade Schwartz*.
[902] Ibid.*Prosser Wade Schwartz*.
[903] Court of Appeals of New York, March 14, 1916. In this case, it was a car whose wheel broke, thus damaging the customer. The defendant was the car manufacturer and not the car retailer. It is interesting also to notice that in this case Judge Cardozo also made reference to English cases on similar issues.
[904] Derrick Owles, and Anthea Worsdall, *Product Liability Casebook. US and UK judgments and commentaries*, (Cholchester; Lloyd's of London Press Ltd, 1984) 1, hereinafter *Owles and Wordsall*.

unexpectedly) then the doctrine of *re ipsa loquitur*[905] could also be applied to breach of duties of care[906].

Moreover, after WWII, judges started to be interested in the concepts of probability and risk, which could be applied not only to economic policy, but also to law. As an example, in 1947, Judge Learned Hand showed a distinct interest in the integration of probability in the evaluation of whether the alleged defendant had been negligent in the famous *United States v. Carrol Towing Co*[907]*.* In the case in hand, a barge had sunk in the North River, dispersing a load of flour belonging to the United States. The United States administration sued the barge company (*Carrol Towing*) because of their negligence in the maintenance the boat, which belonged to yet another party (*Conners Co.*). Judge Learned Hand argued that the probability that a vessel could break from her moorings had to be calculated in the following way : if we call the probability of the boat breaking away P, and the seriousness of the consequent injury L, and the burden of adequate precautions B, then, "[…] *liability depends upon whether B is less than L multiplied by P; i.e., whether B is less than PL (B< P x L)*."[908]

This formula survived the 1940s and would be discussed until a much later date by scholars who are more prone to an economic vision of tort law, such as Calabresi, and others who are instead reluctant to do so, such as Fletcher.

2.1.2. The "attack" on privity[909]: from the implied merchantability warranty to the Uniform Commercial Code

Put very simply, privity is the idea that "[…] *an agreement between A and B cannot be sued upon by C, even though C would be benefited by the performance*."[910] It is the common law equivalent of the continental theories concerning the relativity of the effects of the contract. The respect of privity of contract as a legal rule started in England and one of the most representative cases of this line of thought was *Winterbottom v. Right*[911]. In this famous case, the English courts decided that the plaintiff, a mail coach driver, who had suffered injuries because of an unsafe coach, could not be compensated because he was not a party to the contract passed between the defendant, Mr Wright, a coach manufacturer and repairer, and the Postmaster. The contract's subject was the promise made by Mr Wright to maintain the mail coaches in a safe and secure state. In Lord Alderson's words, if courts had to allow that a person who was not

---

[905] The theory of *res ipsa loquitur* shifts the burden of proof, but only when the defendant had an exclusive control over the product that caused the harm, and the accident could not have happened without negligence. *Owles and Wordsall*, 9.
[906] *Owles and Wordsall*, 9.
[907] *Prosser Wade Schwartz*, 141 & ff.
[908] *Prosser Wade Schwartz*, 141.
[909] The name of this subsection is inspired by Professor Prosser's seminal article where he compares the doctrine of privity to a citadel under attack by the extensive interpretation of judges about strict liability. William L. Prosser, "The Assault upon the Citadel (Strict Liability to the Consumer)," *Yale Law Journal* 69,7(1960): 1099-1148.
[910] Jesse W. Lilienthal, "Privity of Contract," *Harvard Law Review* 1,5 (1887):226. Hereinafter, *Lilienthal*.
[911] *Winterbottom v. Wright*, Exchequer of Pleas, 1842, 10 M. & W. 109, 152 Eng. Rep. *Prosser Wade and Schwartz*, 402 &ff.

privy to a contract be compensated for a damage caused by one of the parties of the original contract "[…] *there is no point at which such actions would stop*" [912]. This was the most practical of the several reasons brought by the court. But there were others, equally important, which were connected to the customs and ideologies of an early capitalist society[913]. In particular, the concept of the contract as meetings of free and autonomous minds would have been compromised[914]. As Lord Abinger stated in his opinion on the same case, by allowing this kind of action, the court would commit an injustice if "[…] *after the defendant had done everything to the satisfaction of his employer, and after all matters between them been adjusted* […], *we should subject them to be ripped open by this action*." [915] The fact that the plaintiff had suffered severe injuries was not an influential enough factor, and, as Lord Rolfe stated "[…] *it is, no doubt, a hardship upon the plaintiff to be without a remedy, but by that consideration we ought not to be influenced. Hard cases, it has been frequently observed, are apt to introduce bad law*."[916]

Nevertheless, already in the 19th century in the US, the New York Court of Appeals decided to go against this limitation in the cases *Lawrence v. Fox*[917] and *Burr v. Beers*[918], also causing a rather scandalised reaction from legal scholars, such as Lilienthal, who defined this way of proceeding, "*the New York rule*", as an "*anomaly*"[919]. The legal instrument that judges started to use all over the US for damages originated from the use of an object (such as an industrial machine and, later, a mass-produced product) was the breach of warranty against the seller[920].

This action was actually created as a remedy of tort, being even older than a special assumpsit[921], the latter being an action which allowed damages due to a breach or non-performance of an oral or written contract, express or implicit, to be recovered[922]. The assumpsit could be common, founded on an implicit promise or special, founded on an explicit one[923]. The warranty action was connected to the writ of trespass from its origin, even if the expression "*warrantizando vendidit*" was conveying the same notion of undertaking as "*super se assumpsit*", the words which generally indicated the writ of assumpsit[924]. The equivalence of assumpsit with a breach of an express warranty in a contract of

[912] *Prosser Wade and Schwartz*, 403.
[913] *Prosser Wade and Schwartz*, 402-403.
[914] *Prosser Wade and Schwartz*, 402-403.
[915] *Prosser Wade and Schwartz*, 402.
[916] *Prosser Wade and Schwartz*, 403.
[917] *Lawrence v. Fox*, N.Y. 268 in *Lilienthal*, 226.
[918] *Burr v. Beers*, 24 N.Y. 178 in *Lilienthal*, 226.
[919] Jesse W. Lilienthal, "Privity of Contract," *Harvard Law Review* 1,5 (1887): 229
[920] To know more about the US selective and creative use of UK product liability case law, see Karl N. Llwelyn, "On Warranty of Quality and Society," *Columbia Law Review* 36,5(1936): 732- 737.
[921] James Barr Ames, "The History of Assumpsit," *Harvard Law Review* 2, 1 (1888):8.
[922] Encyclopædia Britannica, "Assumpsit", 1911, v.2, Accessed 31 January 2023, https://en.wikisource.org/wiki/1911_Encyclop%C3%A6dia_Britannica/Assumpsit. Hereinafter *Assumpsit Definition*.
[923] *Assumpsit Definition*.
[924] James Barr Ames,"The History of Assumpsit," *Harvard Law Review* 2, 1 (1888):8.

sale was what happened in *Stuart v. Wilkins*[925]. Over the course of more than a century, warranties became implied or express terms of contract although they have not lost all connections with tort law. The main feature of the warranty of sale was that the seller had failed to deliver what they had promised[926].

In the case *Baxter v. Ford Motor Co.*[927], Mr Baxter sued both a Ford car retailer, St Johns Motors, and the manufacturer, Ford Motor Company. He alleged that when he had bought the car, both the retailer and manufacturer had advertised the car as having a windshield made of shatterproof glass[928]. Unfortunately, a pebble from a passing car had shattered a piece of windshield which had caused Mr Baxter to lose his right eye[929]. Judge Herman made reference to how society had changed since the rule of *caveat emptor* was first formulated and, that "methods of doing business" - in particular the advent of advertising through radio or billboards - played an important role in creating more demands for product by the consumer[930]. Hence "[…] *it would be unjust to recognize a rule that would permit manufacturers to create a demand for their products by representing that they possess qualities which they, in fact do not possess, and then, because there is no privity of contract existing between the consumer and the manufacturer, deny the consumer the right to recover if damages result from the absence of those qualities, when such absence is not readily noticeable*."[931] In *Baxter v. Ford Motor Co*., the warranty was explicit as both the retailer had advertised the windshield as made of shatterproof glass and the manufacturer had made catalogues claiming the same.

The first seminal case in the US in which an implicit warranty was used in this kind of triangular relationship (two parties tied by contract and a third that had suffered damages or loss because of the contract of the abovementioned parties) was *Henningsen v. Bloomfield Motors Inc.*[932] In this case, Mr Henningsen was injured while driving his car, a 1955 Plymouth automobile model, manufactured by Chrysler Corporation and sold to him by Bloomfield Motors, a car dealer[933]. At the moment of the sale, Mr Henningsen omitted to read the outright majority of the contract, including the terms relating to warranty[934]. The warranty clause excluded any warranty, expressed or implied by the manufacturer or the dealer[935]. The only exception concerned any parts of the car which would turn out to be defective if, and only if, alternatively, i) any part of the car became ineffective within 90 days from the purchase or ii) whether the defect

925 *Stuart v. Wilkins*, 1 Doug 18, 99 Eng. Rep. 15(1778). *Prosser Wade and Schwartz*, 717.
926 G.C.L., "The implied Warranty of Merchantability. Smith v. Hensley," *Virginia Law Review* 48, 1(1962): 153.
927 *Baxter v. Ford Motor Co.* Supreme Court of Washington, 1932. 168 Wash. 456, 12 P.2d 409, *Prosser Wade Schwartz*, 718-722.
928 *Prosser Wade Schwartz*, 718-722.
929 *Prosser Wade Schwartz*, 718-722.
930 *Prosser Wade Schwartz*, 718-722.
931 *Prosser Wade and Schwartz*, 718-722.
932 *Henningsen v. Bloomfield Motors Inc.*, Supreme Court of New Jersey, 1960. 32 N.J. 358, 161, A.2d 69. *Prosser Wade and Schwartz*, 722-728.
933 *Prosser Wade and Schwartz*, 722-728.
934 *Prosser Wade and Schwartz*, 722-728.
935 *Prosser Wade and Schwartz*, 722-728.

was discovered before the car was driven for 4000 miles[936]. Of these two alternatives, the customer was obliged to use the one which happened first[937]. In order to better understand the opinion of Judge Francis, it must also be remembered that in 1906 the Uniform Sales Act already existed, a model law which, if adopted by the single states, imposed some obligations on sellers. Despite the fact that courts had interpreted this federal act in a liberal way, like a protective "cloak" for the buyer (the words of Judge Francis), manufacturers started shielding themselves from liability for their defective products through networks of independent sellers.[938]

Reading the judgment, it is interesting to analyse how Judge Francis reconstructed how the way of contracting had recently changed. If at the beginning the contract had been a meeting and bargain of free minds, it had rapidly become an imbalanced act, where the manufacturer or retailer imposed on consumer contracts, to which the latter had no choice but to accept or not accept the conditions imposed to them[939]. The "[…] *task of the judiciary is to administer the spirit as well as the letter of the law. On issues such as the present one, part of the burden is to protect the ordinary man against the loss of important rights through what, in effect, is a unilateral act of the manufacturer*."[940]

The evolution of the implied and express warranties became part of applicable law with the inclusion of the warranties of merchantability in the Uniform Commercial Code (UCC) in 1952[941]. Article 2 of the UCC contains the warranty provisions and has been implemented in all states. While the rules on implied merchantability warranty are similar to the former Uniform Sales Act (§§ 2-314 and 315), the code has also extended warranties to third parties[942]. Each state is free to choose from three alternatives[943]. The third parties covered by the alternatives are the following: "*A) the buyer's family members or house guests B) any natural person who might be reasonably expected to use or consume or be affected by the goods and is injured by breach of warranty or C) any person who may reasonably be expected to use consume or be affected by the goods and who is injured by breach of warranty*"[944]. In this case, the seller may not exclude or limit the operation of this section with respect to injury to the person of an individual to whom the warranty extends. It must be remembered that, although influential, adoption of the UCC remains optional. Therefore, from an EU point of view it would seem that the UCC is an instrument of harmonization more akin to a minimum harmonization directive than to a regulation[945]. Despite codification, the percentage of judgments using the warranty scheme (also from the UCC) was

[936] *Prosser Wade and Schwartz*, 722-728.
[937] *Prosser Wade and Schwartz*, 722-728.
[938] *Prosser Wade and Schwartz* ,722.
[939] *Prosser Wade and Schwartz*, 724-726.
[940] *Prosser Wade and Schwartz*, 726.
[941] *Prosser Wade and Schwartz*, 724-728
[942] *Prosser Wade and Schwartz,* 724-728.
[943] *Prosser Wade and Schwartz*, 727-728.
[944] *Prosser Wade and Schwartz*, 727-728.
[945] For an interesting discussion concerning the influence of the UCC over products liability cases, see Marc A. Franklin, " When Worlds Collide: Liability Theories and Disclaimers in the Defective-Product Cases," *Stanford Law Review* 18,6 (1966): 974-1020.

not as high as one continental lawyer would expect: in fact, it used to be below 3% threshold of the cases which could be labelled as in some way connected to products liability[946].

2.1.3. 1963: The strict liability doctrine and its influence on the Restatement Second of Torts

1963 was a pivotal year for products liability in the US[947]. It was a culmination of decades of debate around the protection of consumers against defective products. Two major events established a new theory, called strict liability, applied to products liability in those years[948].

The first was a judgment of the Supreme Court of California in 1963, known as *Greenman v. Yuba Power Products Inc*[949]. In this case, Mr Greenman injured himself while using a Shopsmith, a tool that could be used as a saw, drill or wood lathe[950]. Ten and a half months after the accident, Greenman contacted both the retailer and the manufacturer, claiming that the product infringed both expressed and implicit warranties[951]. The plaintiff argued by relying on documentation that the design of the object was defective overall[952]. Nevertheless, the defendant argued that these claims could not be accepted as the consumer had not given notice of the damage he had suffered within a reasonable time, hence the plaintiff was time barred, according to the rules of the California Civil Code[953]. Judge Traynor, however, considered that recalling civil law rules was not pertinent in that case, where there had been bodily injuries[954]. According to Judge Traynor "[…a] *manufacturer is strictly liable in tort when an article he places on the market, knowing that it has to be used without inspection for defects, proves to have a defect that causes injury to a human being.* […] *Although these cases of strict liability have usually been based on a theory of an express or implied warranty running from manufacture to the plaintiff, the abandonment of the requirement of a contract between them, the recognition that the liability is not assumed by agreement but imposed by law* […] *and the refusal to permit the manufacturer to define the scope of his own responsibility for defective products* […] *make clear that the liability is not one generated by the law of contract warranties but by the law of strict liability in tort*." [955] Hence, the judiciary developed a new form of

[946] Michel Cannarsa, *LA RESPONSABILITÉ DU FAIT DES PRODUITS DÉFECTUEUX. ÉTUDE COMPARATIVE*, (Milano:Giuffrè editore, 2005),36.
[947] Michael Green and Jonathan Cardi, "Product Liability in the United States of America," in *European Product Liability: An Analysis of the State of the Art in the Era of New Technologies*, Piotr Machnikowski (Cambridge, Portland Antwerp: Intersentia, 2016) 576. Hereinafter *Green and Cardi*.
[948] Strict liability as such already existed as part of negligence and tort law in the US, and like in other continental law countries, it concerned mostly animals and inherently dangerous activities. See Chapter IV, subsection 1.1.2., II.
[949] *Greenman v. Yuba Power Products, Inc.* Supreme Court of California, 1963, 59 Cal.2d 57, 377 P. 2d 897, 27 Cal. Rptr 697. *Prosser Wade and Schwartz*, 729.
[950] *Prosser Wade and Schwartz*, 729-730.
[951] *Prosser Wade and Schwartz*, 729-730.
[952] *Prosser Wade and Schwartz* ,730.
[953] *Prosser Wade and Schwartz*, 730-731.
[954] *Prosser Wade and Schwartz*, 731.
[955] *Prosser Wade and Schwartz*,732.

liability from negligence that did not require fault to be proved by the complainant in order for them to succeed. This was possible provided that certain conditions were met. In *Greenman,* Judge Traynor claimed that it was sufficient for the complainant to prove that he had sustained injuries while using the product in a way in which the object had been created to be used and as a result of a design defect and manufacture of which the plaintiff was not aware and that made the product unsafe[956].

This judgment was highly influential as it stated that strict liability in tort could be applied to mass-produced objects. This facilitated acceptance by legal scholars who had endorsed the liberal views of the judiciary vis-à-vis consumer protection through strict liability. They integrated these principles in the 1965 Restatement Second of Torts[957]. In particular, it was Section 402 a) that condensed the jurisprudence evolution of many years. To provide a better analysis, I will copy the text of Section 402 A) entitled Special Liability of the Seller of Product for Physical Harm to User or Consumer

> *(1) One who sells any product in a defective condition unreasonably dangerous to the user or consumer or to his property is subject to liability for physical harm thereby caused to the ultimate user or consumer, or to his property, if*
> *(a) the seller is engaged in the business of selling such a product, and*
> *(b) it is expected to and does reach the user or consumer without substantial change in the condition in which it is sold*
> *(2) The rule stated in subsection (1) applies although*
> *(a) the seller has exercised all possible care in the preparation and sale of his product, and*
> (b) *the user or consumer has not bought the product from or entered into any contractual relation with the seller*. [958]

The definition of defect that was given in the Restatement second, and in particular the concept of defect as a condition that is unreasonably dangerous to consumer inspired Article 6(1) PLD. Even though illustrious American commentators have identified this part of the Restatement Second as proof that the EU PLD was a replica of the American Restatement Second[959], I believe that the situation is more nuanced. It is true that the consumer's expectation test was taken as a reference in the PLD, but already in Article 6 PLD there are differences that render the EU product liability system a system that is inspired by American case law and legal doctrine of the early 1960s, but not a mere copy of it.

---

[956] *Prosser Wade and Schwartz*, 732.
[957] The function of a Restatement, which is curated by the American Law Institute (ALI), is to provide consensus over legal issues discussed by courts and scholars. Michael Green and Jonathan Cardi, "Product Liability in the United States of America," in *European Product Liability: An Analysis of the State of the Art in the Era of New Technologies*, Piotr Machnikowski (Cambridge, Portland Antwerp: Intersentia, 2016), 581.
[958] *Prosser Wade and Schwartz*, 733.
[959] *Prosser Wade and Schwartz* , 733.

To begin with, one of the main differences of the PLD article is that it details what should influence the consumer's expectation about the ordinary safety of a product by giving a list of indicative suggestions. Furthermore, one other main point of difference with the PLD concern the subjects from which the user-consumer can actually ask for compensation. In the restatement in the US, only the vendor and the distributor are mentioned[960], however, there is the possibility that other subjects such as the manufacturer could be apportioned liability and comparative responsibility rules are employed.[961] On the contrary, in the PLD the producer is in principle the only liable subject. And, in the lexicon of the PLD, producer actually means the manufacturer of the final product, according to Article 3(1) PLD. Only when it is not possible to identify the producer, states Article 3(3) PLD, it is possible that liability shifts to other meaningful members of the supply and value chain. As far as apportionment of liability, Article 5 PLD and the jurisprudence cited in Chapter 5, among which the recent *Fennia* case[962], states that the consumer chooses whoever presents itself as producer in order to recover damage. If there are many stakeholders involved, it would be a matter of national law to establish recovery actions for the producer who paid for the damage caused (also) by other subjects. Finally, the rules on damage are more general in the restatement and there are no conditions, as in Article 9,(b),(i) and (ii) to limit the damage on private property. Moreover, the only physical damage that is covered in section 402 A) is physical harm, although it has been established by case law that also pecuniary loss deriving from physical harm could be obtained through damages[963]. With the PLD, death and personal injuries are covered by Article 9 (a) and, according to *Veedfald* judgment, the MS are free to also compensate for immaterial damage caused by the defective product (see Chapter V). Finally, in 402 A (2),(a), not even when the seller has exercised all the possible care is he exempted from liability. Theoretically, according to the PLD the producer has six exemptions listed in Article 7 PLD that, although difficult to prove, are in principle a legal instrument that balances the PLD as a regulatory set of rules rather than a consumer protection set. The reason for these many differences is that matters changed in the US after the introduction of the Restatement Second on Torts and the EU, then the EC, also took inspiration from the changes in jurisprudence and in legal expertise that followed. (for more on this see sub-section 1.1.4.)

2.1.4. New defects under the Restatement Third of Torts, and products liability to the present day.

One of the main innovations brought by Section 402 A) was a unique and very broad definition of damage[964]. Moreover, the consumer expectation test was also considered to be difficult to apply in certain circumstances: for instance,

[960] *Prosser Wade and Schwartz* , 593-594.
[961] *Green and Cardi*, 594-596.
[962] Chapter 5 Article 3 PLD, subsection 3.1.2.
[963] *Prosser Wade and Schwartz*, 796.
[964] *Prosser Wade and Schwartz*, 735.

when the product is obviously dangerous, a consumer cannot not have any safety expectations and, especially when the defect concerned an object's design, there were no common safety expectations, especially in complex objects[965]. All, in all, as summarily put by Professor Brinbaum, the source of problems in identifying a defect and in finding a way for the plaintiff to prove it came from "[…] *the dual legacy of Greenman, on the one hand, with its singularly bald notion of product defect, and section 402A on the other, with its amorphous terminology 'defective condition unreasonably dangerous'*."[966] Hence, through a series of landmark cases, three main types of damages were actually stabilised in judicial practice and also in theoretical discussions. These judicial but also theoretical discussions accumulated until 1998 and they gave rise to a new Restatement, the Restatement Third of Torts.

The first type of defect was a manufacturing defect. This is a defect that pertains to the object alone, and not to all the product lines, hence the rules of *Greenman* and the Restatement Second could be applied without much controversy. This was the outcome of *Rix v. General Motor Corps*[967]. The second kind of defect is a design defect. This one is the most difficult to ascertain as, as stated in *Caterpillar Tractor Co. v. Beck*[968], if to assess the defectiveness based on malfunctioning, one had the design of the product that needed to be taken into account as reference, it was not the case for the design defect where there was not an objective point of reference[969]. *Prentis v. Yale Mfg. Co*.[970] also gives an account of the heated discussion concerning how to identify the design defect. In particular, in this case Justice Boyle recalls the different theoretical standards available at that time in order to ascertain the existence of a design defect. Dean Wade used a risk analysis approach, whereas Dean Keeton compared the risk and utility of the product at the time of the trial[971]. A third criterion concerned consumer expectations and a last one combined the consumer expectation and risk utility test.[972] In the end, the court adopted the approach of negligence to prove the design defect, by following the indications of the Model Uniform Product Liability Act (UPLA) of 1979 and Professor Birnbaum's theses on the matter, meaning that the rules on negligence had to be used[973]. This also appeared justifiable in terms of industrial policy and allocation of risks: the UPLA maintained that design defects"[…] *originate from deliberate and documentable decisions*… [and a] *greater incentive in designing safer products will result from a fault system where resources devoted to careful and safe design will pay dividends in form of fewer claims*…[moreover] *the verdict for the plaintiff in a*

[965] Jerry J. Phillips and Robert E. Pryor, *Products liability Volume I* (Wolters Kluwer Products liability Library, 1993, 2nd ed.), 20.
[966] Sheila L. Birnbaum, "Unmasking the Test for Design Defect: From Negligence [to Warranty] to Strict Liability to Negligence," *Vanderbilt Law Review* 33, 3(1980):599.
[967] *Rix v. General Motors Corp*., Supreme Court of Montana, 1986. 222 Mont. 318,723 P.2d 195, *Prosser Wade and Schwartz*, 737.
[968] *Caterpillar Tractor v. Beck*, 593 P.2d 871, 880, Alaska 1979. *Prosser Wade and Schwartz*, 746.
[969] *Prosser Wade and Schwartz*, 746.
[970] *Prentis v. Yale Mfg. Co.*, Supreme Court of Michigan, 1984. 421 Mich. 670, 365 N.W. 2d 176, *Prosser Wade and Schwartz*, 740 &ff.
[971] *Prosser Wade and Schwartz*, 740 &ff.
[972] *Prosser Wade and Schwartz*, 742.
[973] *Prosser Wade and Schwartz*, 743.

design defect case is the equivalent of a determination that an entire product line is defective […] *Thus the plaintiff should be required to pass a higher threshold of a fault test in order to threaten an entire product line.*"[974]

However, in another case, *O'Brien v Muskin Corp.*[975], it was the risk utility test that was used in order to demonstrate the presence of the defect, and that was also the criteria followed by most courts[976]. Most probably, one of the reasons for the success of this criterion was its connection to negligence and fault, which was possible through an ideal comparison with a state of the art at the time of the product being marketed[977] and that was used as a term of reference to demonstrate the design defect.

The third kind of defect is the one concerning warnings and information. In *Anderson v. Owens- Corning Fiberglas Corp.*[978] Justice Panelli made a complex distinction about what the differences were concerning the failure to warn of both according to negligence and to strict liability[979]. In the case at hand, it was discussed whether a defendant in a products liability action based on a failure to warn of a certain harm risk, could actually defend themselves by presenting evidence that it was neither known or knowable at the time of manufacture or distribution according to the state of the art at that time[980]. Panelli argued that a reasonably prudent manufacturer might decide that the risk of harm is not so high as to deserve a warning, even if the scientific community says otherwise[981]. Under negligence rules they could be exempted from liability but not under strict liability rules[982]. Hence "[…] *the failure to warn theory of strict liability compels the conclusion that knowability is relevant to the imposition of liability under that theory*"[983]. However, Panelli states that despite the recognition of the principle that strict liability is important in order "[…] *to spread the risks on the ones who could bear them* […] *it was never the intention of the drafters of the doctrine to make the manufacturer or distributor the insurer of the safety of their products. It was never their intention to impose absolute liability*".[984] This case is interesting as it reconnects with the idea of the exemption for risk development which can be found in Article 7(e) PLD.

In order to clarify matters, from 1993 to 1998 the American Law Institute (ALI) worked on the Restatement Third of Torts which specifically treated products liability[985]. The main innovations were the change of structure in the liability definition. The new §1, entitled Liability of the commercial seller or

[974] *Prosser Wade and Schwartz*,743-744.
[975] *O'Brien v Muskin Corp.* Supreme Court of New Jersey, 1983. 94 N.J. 169, 463 A 2d 298. *Prosser Wade and Schwartz.*
[976] *Prosser Wade and Schwartz*, 750-752.
[977] *Prosser Wade and Schwartz*, 750.
[978] *Anderson v. Owens- Corning Fiberglas Corp*. Supreme Court of California, 1991. 53 Cal3d, 810 P.2d 549, 281 Cal. Rptr.528. *Prosser Wade and Schwartz*, 755-764.
[979] *Prosser Wade and Schwartz*, 755-756.
[980] *Prosser Wade and Schwartz*, 755-756.
[981] *Prosser Wade and Schwartz*, 755-758.
[982] *Prosser Wade and Schwartz*, 758.
[983] *Prosser Wade and Schwartz*. 758-759.
[984] *Prosser Wade and Schwartz*, 759.
[985] *Prosser Wade and Schwartz,* 736.

distributor for harm caused by defective products loses the expression “defective condition unreasonably dangerous” of the previous section 402 A in favour of the more neutral and concise:

> (a) *One engaged in the business of selling or otherwise distributing products who sells or distribute a defective product is subject to liability for harm to person or property caused by the defect*.

Then § 2 describes the 3 main kinds of defects which are the same as the ones highlighted *supra*. The standard for which all three defects must be evaluated is the one of the risk-utility test, which is carried out by applying Judge Learned Hand’s formula[986]. For the manufacturing defect, the point of reference is how it differs from the original design and not even the maximum level of care could be used as grounds for an exemption[987]. With regard to the design defect, the proof for the plaintiff is to demonstrate that the damage would not have happened were the manufacturer to adopt an alternative design[988]. This means that the risk utility test is the sole criterion that is used for evaluating the safety of a design[989]. It employs a cost-benefit methodology to take into account additional safety that could be possible if the design were different[990]. It could rely on the costs that might implicate issues that are non-economic, such as functionality, aesthetics and other elements such as safety in personal injury that are not easily quantifiable[991]. The same could be stated for the warning defects: a defect in this case consists of inadequate instructions, that had they been complete, could reduce the risk of harm posed by the product or their omission[992].

In summary, nowadays in the US there are several approaches to product liability: there is still negligence, which reappeared with the design defectiveness concept; there are national rules on implied or express merchantability warranties of the UCC, if the State has implemented the relative UCC article on those warranties; there is strict liability which depends on statutes or on judgments and, we will see in chapter 2, other statutes, both national and federal, that could be playing a role. This paragraph, with all its subparts, had the role of clarifying the historical main steps that contributed to the actual asset of an ensemble of different rules that can be synthesised with the expression products liability. I will try to discover in the next part of this first section of the chapter, whether the growing importance of technology is going to influence regulation (2.2) and, if so, if it has any consequences on products liability.

2.2. US priorities in technology regulation: platforms, AI and the IoT

[986] See subparagraph 1.1.1. of this chapter and *Green and Cardi*, 587
[987] §2(a) *Prosser Wade and Schwartz*, 737.
[988] *Green and Cardi*, 587.
[989] *Green and Cardi*, 587.
[990] *Green and Cardi*, 587.
[991] *Green and Cardi*, 587.
[992] *Green and Cardi*, 587 &ff.

Traditionally, the US has always been a nation which believed in the self-regulation of the market, even when it came to new technologies[993]. The Internet made no exception, if considered as a final result of several sets of different technologies[994]. Besides, this approach gave rise to some of the private companies without which our life would not be the same, such as Google, Apple, Microsoft, Amazon and the Meta group. Moreover, the first meeting of scientists which formally started the studies on AI was also held in the US, at Dartmouth college, in 1956[995].

It would seem, then, that a permissive take on the activities of technological companies is what is required to have a global leadership position in this field. Despite this, many scholars from the field of sociology, politics and law have been warning the general public for years about the surveillance aspects that new technologies have on our lives: it is no secret that the data that consumers and users exchange to get goods and services is used by private corporations to make their services better[996]. These corporations may as well collaborate with public authorities both at a national and at a federal level for different purposes[997]. However, firstly in the EU, but now also in the US, there are growing governmental concerns over the benefits of this approach in the long term. For some time, even in the US, there has been a lively debate about the necessity to split up the big Internet corporations as their role in economy raised concerns from the point of view of antitrust law[998]. This kind of scenario invites

[993] Nicholas Davis, Mark Esposito and Landry Signé, "The anatomy of technological regulation," *Brookings*, February 17, 2022, https://www.brookings.edu/opinions/the-anatomy-of-technology-regulation/ .
[994] See Chapters II and IV.
[995] "Artificial Intelligence (AI) Coined at Dartmouth," *Dartmouth (*official website), https://250.dartmouth.edu/highlights/artificial-intelligence-ai-coined-dartmouth .
[996] Especially, the power of unexplainable algorithms in our lives and the economy that depends on it has been explained by Frank Pasquale and Solon Barocas and Andrew D. Selbst among many. See Frank Pasquale, *The Black Box Society*, (Cambridge-Massachussets, London: Harvard University Press, 2015), and Solon Barocas and Andrew D. Selbst, "Big Data's Disparate Impact," *California Law Review* 104 (2016): 671-732. The literature on cybersurveillance is indeed quite extensive and I do not wish to enter into this debate. I can only suggest the reading of Shoshana Zuboff's main work, called The Age of Surveillance Capitalism. Shoshana Zuboff, *The Age of Surveillance Capitalism: the Fight for a Human Future at the New Frontier of Power*, London: Profile Books, 2019.
[997] One example can illustrate these concerns better. After the overturn of *Roe v. Wade* in June 2022, the judgment which protected abortion at a federal level, some states started implementing severe laws towards people who get or help to seek abortion healthcare services. Digital activists had warned that digital period trackers and social media could give access to customers' reproductive health data to government authorities finalised to criminal prosecution. These concerns became reality on 10th August when it was reported that Meta group had given Nebraska police access to private direct messages (DM) exchanged through Facebook's Messenger chat service between a minor seeking an abortion pill and her mother in Nebraska. Now the two women faces criminal charges under the abortion law of that state. "Nebraska mother, teenager face charges in teens abortion after police obtain their Facebook DMs", CBS Bay Area- Technology, August 10, 2022, https://www.cbsnews.com/sanfrancisco/news/facebook-nebraska-abortion-police-warrant-messages-celeste-jessica-burgess-madison-county/; Zoe Kleinman," The abortion privacy dangers in period trackers and apps," BBC News, June 28, 2022, https://www.bbc.com/news/technology-61952794 .
[998] Astead W. Herndon, "Elizabeth Warren Proposes Breaking Up Tech Giants Like Amazon and Facebook," *The New York Times*, March 8, 2019, https://www.nytimes.com/2019/03/08/us/politics/elizabeth-warren-amazon.html. Konstantinos Efstathiou, " Breaking up big companies and market power concerntration," *bruegel*, April 29, 2019, https://www.bruegel.org/blog-post/breaking-big-companies-and-market-power-concentration. Toria Rainey, "Is Breaking Up Amazon, Facebook, and Google a Good Idea?," *Boston University Today*, October 7, 2019, https://www.bu.edu/articles/2019/break-up-big-tech/.

comparisons with what happened at the end of the XIX century with the case *Standard Oil*, the "dawn" of antitrust law (or competition law, in EU legal parlance).

Indeed, it seems that antitrust law is the favourite regulatory and legislative instrument to tackle the market (and not only) power of corporations. At the moment of writing, the US congress is trying to pass the "American Innovation and Choice Act,"[999] which both Republicans and Democrats support. If passed, this bill will regulate the market power of some of the most influent digital companies, most of which are platforms[1000] but also search engines. From a first reading of the draft and comments, it seems that this bill took Article 2 DMA's definition about core platform services (in the American equivalent online platform[1001] and covered platform[1002]) and Article 3 DMA's gatekeepers definition and way of application as references. The American bill targets companies of a certain size or global reach with a certain revenue and with a significant tie to the US economy [1003]. Then, in Section 3 of the American and Innovation Choice Act, there is a list of practices which will be prohibited and that could be further described which is self-explanatorily named "Unlawful Conduct". This section is also clearly inspired by Article 5 and 6 DMA. For instance, this part of the bill bans practices such as self-preferencing[1004] of the same platform's products or services, such as in Article 6 DMA. The covered platform could use some affirmative defences against the Federal Trade Commission (FTC), whereas in the DMA, if the Commission finds the core service platform liable for enacting one of the behaviours in Article 5 and 6 DMA, there are no specific self-defences but rebuttable presumptions. In the EU regulation, the gatekeeper could also apply for a suspension or exemption from the application from said articles 5 and 6 DMA according to Articles 8 and 9 of the DMA. The result of the EU procedure under the DMA could be a fine according to the rules of Articles 26 and 27 DMA. This is an administrative act which could be contested before the CJEU. In the American Innovation and Choice Act, the procedure is the one followed before the FTC with the provision of civil penalty, and, when necessary, equity relief.

If this bill had been approved before the November 2022 mid-term elections, it would surely have been the greatest attempt at Internet Regulation ever.

Search engines and platforms are multi-level technological stakeholders but also economic and political players, therefore it is understandable why regulation through antitrust might obtain bipartisan support. The situation is not the same concerning other "purer" forms of technology which employed more time to get support compared to the "American Innovation and Choice Act". AI has received more recent attention than the IoT and, like in the EU, it would

[999] S.2992- American Innovation and Choice Online Act. Sponsor: Sen, Klobuchar, Amy, Senate, Accessed 31 January 2023, https://www.congress.gov/bill/117th-congress/senate-bill/2992/text. Hereinafter American Innovation and Choice Online Act.
[1000] See definition n.9 "Online Platform", American Innovation and Choice Online Act.
[1001] See definition n.9 "Online Platform", American Innovation and Choice Online Act
[1002] See definition n. 5 "Covered platform", American Innovation and Choice Online Act.
[1003] See definition n. 5 "Covered platform", American Innovation and Choice Online Act.
[1004] See definition Section 3 Unlawful conduct (2) self-preferencing and see Article 6(d) DMA.

appear that the rationales underpinning the two approaches have started to align[1005], maybe also as a consequence of the enactment of the U.S.–EU Trade and Technology council, a new technology partnership between the two parties[1006].

In 2021, the Good AI act[1007] was sent to Congress to be discussed. The scope of this proposed act is to set principles and policies for the use of AI in government services (section 2) and also the creation of the Artificial Intelligence Hygiene Working Group, similar to the AI High Level Expert Group (AI-HLEG) which wrote the Ethical Guidelines for a Trustworthy AI in 2019. The American Good AI act makes reference to the John McCain Bill for the Fiscal Year 2019 with regard to the definition of AI, which mostly coincides with machine learning algorithms[1008]. The Good AI act, like the EU AI act, contains a definition of AI system which

"(*A) means any data system, software, application, tool, or utility that operates in whole or in part using dynamic or static machine learning algorithms or other forms of artificial intelligence, including a data system, software, application, tool, or utility—*

(i) that is established primarily for the purpose of researching, developing, or implementing artificial intelligence technology; and

(ii) for which the artificial intelligence capability is integrated into another system or agency business process, operational activity, or technology system; and

(B) does not include any common or commercial product within which artificial intelligence is embedded, such as a word processor or map navigation system."

Hence, if we consider part (B) of the definition, an AI system formally excludes IoT objects, especially domestic IoT objects, for which more refined AI algorithms are being integrated into the device or within the cloud at an increasing rate[1009].

[1005] Alex Engler, "The EU and U.S. are starting to align on AI regulation," *Brookings*, February 1, 2022, https://www.brookings.edu/blog/techtank/2022/02/01/the-eu-and-u-s-are-starting-to-align-on-ai-regulation/ .

[1006]"U.S.- EU Trade and Technology Council Inaugural Joint Statement," The White House, September 29, 2021,Accessed 31 January 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/29/u-s-eu-trade-and-technology-council-inaugural-joint-statement/, and European Commission, " EU-US Trade and Technology Council: strengthening our renewed partnership in turbulent times," EU Commission Press release, May 16, 2022, Accessed 31 January 2023, https://ec.europa.eu/info/strategy/priorities-2019-2024/stronger-europe-world/eu-us-trade-and-technology-council_en.

This would also explain the mirroring of certain initiative on chip manufacturing, such as the EU Chips Act and the US Chips act. See "European Chips Act: Communication Regulation Joint Undertaking and Recommendation." *European Commission*, February 8, 2022, Accessed 31 January 2023, https://digital-strategy.ec.europa.eu/en/policies/european-chips-act , https://www.whitehouse.gov/briefing-room/statements-releases/2022/08/09/fact-sheet-chips-and-science-act-will-lower-costs-create-jobs-strengthen-supply-chains-and-counter-china/.

[1007] S.305-GOOD AI Act of 2021, Sponsor: Sen. Peters, Garty C. introduced 10/21/2021, Accessed 31 January 2023, https://www.congress.gov/bill/117th-congress/senate-bill/3035/text.

[1008] The act makes a reference to meaning of AI to John Mc Cain Bill for fiscal year 2019, section 238 g https://www.govinfo.gov/content/pkg/CRPT-115hrpt874/pdf/CRPT-115hrpt874.pdf .

[1009] See Chapter II.

This is interesting as the US government seems to separate regulations for the IoT and the AI domain[1010]. The EU approach is more ambiguous, as we have seen in Chapter III: there are several legislative acts and proposed legislative acts (such as the Data Act) that are applicable to the IoT, but none of them mention these devices explicitly in their operative parts. Only ENISA, the specialised cybersecurity agency, offered a simple definition of IoT. According to the agency, the IoT is "[…] *a cyber-physical ecosystem of interconnected sensors and actuators which enable intelligent decision making*"[1011]. ENISA also uses this definition when it refers to the IoT in its periodical cybersecurity publications, such as the Threat Landscape reports[1012].

Also in the US, similarly to the EU, the US appears to connect the IoT more with cybersecurity aspects than legal ones. In tackling IoT cybersecurity, there was a gradual approach, starting with soft law in 2015 and culminating with national and federal requirements in 2018 and 2019. For instance, in 2016, the IoT was already in the government action spotlight. This was because IoT cybersecurity weaknesses raised concerns in the Department of Homeland Security, which published a list of strategic principles to secure the IoT[1013]. The IoT received a high level of regulatory attention, especially in the period 2019-2021 both at federal and national level[1014], concerning hard and soft law regulatory instruments. However, this attention only pertains to the cybersecurity aspect and not the product liability one. This thesis does not intend to address the matter of cybersecurity. However, I believe it is important to have a brief summary of what these several initiatives involved, in order to understand how it might affect American products liability theories in the future. In fact, a low level of quality and safety in IoT devices, especially domestic ones, concerning both hardware and software, could be a major cause of damage. As far as soft law is concerned, these claims are also supported by the action of the Federal Trade Commission (FTC)[1015] and other federal agencies such as the Consumer Product Safety Commission (CPSC), which have warned about the risks that these objects might entail for consumers recently. In particular, in January 2019, the CPSC published a Framework of Safety of the Internet of Things, which tried to clarify safety duties for IoT manufacturers mostly based on risk assessment

[1010] As far as the AI matters are concerned, it can be notices that NIST has started elaborating a framework for AI security which also relies on standards, such as, *mutatis mutandis*, the EU AI Act. More on this at NIST, *AI Risk Management Framework. Second Draft*. *August 18 2022*, Accessed 31 January 2023, https://www.nist.gov/system/files/documents/2022/08/18/AI_RMF_2nd_draft.pdf.
[1011] ENISA, *IoT and Smart Infrastructures* (presentation page), Accessed 31 January 2023, https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot .
[1012] ENISA, *Threat and Risk Managment- Publications* (presentation page), Accessed 31 January 2023, https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends?tab=publications .
[1013] U.S. Department of Homeland Security, *Strategic Principles for Securing the Internet of Things Version 1.0*, November 15, 2016, Accessed 31 January 2023, https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf.
[1014] California and Oregon being the first state with a comprehensive cybersecurity framework on cybersecurity See KPMG, *After the rainfall of IoT regulations*, Accessed 31 January 2023, https://advisory.kpmg.us/articles/2020/rainfall-iot-regulations.html and pwc, "Three actions for IoT device manufacturers from the IoT Cybersecurity Improvement Act of 2020", Accessed 31 January 2023, https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/iot-cyber-improvement-act.html.
[1015] More on this in section 2.1.1. of this Chapter.

methods and also identifying possible countermeasures such as certification of IoT components and user authentication requirements[1016]. However, while the CPSC has jurisdiction over the product safety of most consumer goods including the IoT connected devices, it does not generally regulate product safety issues relating to privacy and data security[1017]. These are competences divided between the FTC and the Federal Communications Commission (FCC). The FTC focused its attention on privacy and security of the IoT, publishing a report in 2015 on these themes[1018] and keeping its webpage constantly updated on the issue[1019].

Congress passed the Internet of Things Cybersecurity Improvement Act as federal law in 2020[1020], which should be implemented by the National Institute of Standards and Technology (NIST). This bill contains the particularly interesting definition of IoT devices as devices that:

> "*(A) have **at least one transducer** (sensor or actuator) for interacting directly with the physical world, have **at least one network interface**, and are not conventional Information Technology devices, such as smartphones and laptops, for which the identification and implementation of cybersecurity features is already well understood; and*
>
> *(B) **can function on their own** and are not only able to function when acting as a component of another device, such as a processor*."[1021]

It is an extremely technical definition, even if we compare it with the one used by ENISA (chapter II and III) and also with the product definition in Article 2(2) Data Act. It is also particularly interesting that this definition excludes smartphones, which are technically IoT objects.

Due to the delegation of the Internet of Things Cybersecurity Improvement Act in 2020, the NIST has been working alone to standardise the IoT: it has established the NIST Cybersecurity for IoT devices programme and has issued several guidance documents such as recommendations NISTIR 8259 A[1022] and NISTIR 8259[1023]. The first document identifies a core baseline of IoT device

---

[1016] Elliot F. Kaye and Jonathan D. Midgett for CPSC, " A FRAMEWORK OF SAFETY for the Internet of Things: Considerations for Consumer Products Safety," January 31, 2019, Accessed 31 January 2023, https://www.cpsc.gov/s3fs-public/A_Framework_for_Safety_Across_the_Internet_of_Things_1-31-2019.pdf.

[1017] "Safety Best Practices for IoT Devices," *Practical Law (Westlaw)* (2019):1-14.

[1018] FTC Staff Report, *Internet of Things. Privacy and Security in a Connected World*. January 2015, Accessed 31 January 2023, https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[1019] "Careful Connections: Keeping the Internet of Things Secure," *FTC*, Accessed 31 January 2023, https://www.ftc.gov/business-guidance/resources/careful-connections-keeping-internet-things-secure .

[1020] H.R.1668 - IoT Cybersecurity Improvement Act of 2020, Sponsor Kelly Robin. Accessed 31October 2022, https://www.congress.gov/bill/116th-congress/house-bill/1668/text .

[1021] Emphasis added.

[1022] Michael Fagan, Katerina N. Megas, Karen Scarafone and Matthew Smith, *NISTIR 8259 A IoT Device Cybersecurity Capability Core Baseline*, Nist website, Accessed 31 January 2023, https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259A.pdf.

[1023] Michael Fagan, Katerina N. Megas, Karen Scarfone and Matthew Smith, *NISTIR 8259 Cybersecurity Activities for IoT Device Manufacturers*, NIST website, 2020. Accessed 31 January 2023, https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259.pdf.

cybersecurity for manufacturers, whereas the second document provides a list of recommended actions to make producers able to respond to consumers' needs. Moreover, on 4 February 2022 it also published indications concerning labelling of IoT devices for consumers[1024]. Even though the NIST plays an important role in standardising the cybersecurity aspects of the IoT, at the federal level the FTC might be the only regulator of the IoT and not just concerning cybersecurity. It will be demonstrated that the FTC uses consumer protection instruments to actually address data privacy and data security, which might be connected to the concept of defect of product, hence to products liability. More on this in 2.1.1. below.

Even before the federal government became involved in regulating the IoT, California passed an amendment concerning IoT and privacy in 2018, which only became effective from 1st January 2022. It is the California Bill no. 327 which amends the California Civil Code and adds title 1.81.26 to Part 4 of Division 3 of the Civil Code, relating to information privacy[1025]. This bill does not have a definition of IoT devices *per se,* but of "connected devices". It is a broad definition as it is a "[…] *device, or other physical object that is capable of connecting to the Internet, directly or indirectly, and that is assigned an Internet Protocol address or Bluetooth address*."[1026] Contrarily to EU definitions, which tend to be technologically neutral, the American state legislation also contains a mention of specific technologies, not as an example but as a part of a legal definition, such as the mention of Bluetooth technology. One main difference with the federal definition of IoT is that the Californian one also considers an indirect connection to the Internet as relevant for identifying a connected object. Hence, the California Bill is applicable to a wider range of devices compared with the federal rules on the same subject.

The bill requires manufacturers of connected devices to build the devices or equip them with reasonable security features, deigned to protect the device and its information from unauthorised access, modification or disclosure[1027] and as examples of reasonable security features it lists that they must be: "

1. *Appropriate to the nature and function of the device*

2. *Appropriate to the information it may collect, contain or transmit and*

[1024] NIST, Consumer IoT Cybersecurity. Improving Consumer IoT Cybersecurity, Accessed 31 January 2023, https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/consumer-iot-cybersecurity.

[1025] (California) Senate Bill N 327 Chapter 886, An act to add Title 1.81.26, Accessed 31 January 2023, https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.26.&part=4.&chapter=&article. And White&Case technology Newsflash, "Connected devices: Challenges for both technology providers and consumers," White &Case, May 27, 2019, Accessed 31 January 2023, https://www.whitecase.com/insight-our-thinking/connected-devices-challenges-both-technology-providers-and-consumers.

[1026] 1798.91.05, (b) White &Case, May 27, 2019, Accessed 31 January 2023, https://www.whitecase.com/insight-our-thinking/connected-devices-challenges-both-technology-providers-and-consumers.

[1027] White &Case, May 27, 2019, Accessed 31 January 2023, https://www.whitecase.com/insight-our-thinking/connected-devices-challenges-both-technology-providers-and-consumers .

3. *Designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification or disclosure*"[1028]

This is similar to the principle of privacy by default and by design established in Article 25 GDPR.

According to commentators, however, there are also shortcomings in the law as, firstly, it does not create remedies for consumers[1029]; secondly, the bill does not regulate issues connected to third-party software or applications that a user chooses to install on their device (the EU case of standalone software) and, thirdly, the bill does not require app stores to review or enforce compliance[1030]. Moreover, the connected devices that have to respect security requirements under federal law are excluded from the application field of the bill as well as the devices' activities that are subject to the federal Health Insurance Portability and Accountability Act of 1996 ("HIPAA") or the Confidentiality of Medical Information Act ("CMIA)[1031]. At the very least, the law does not limit the authority of any law enforcement agency to obtain connected device information from a manufacturer[1032].

In summary, the US regulation of technology could be defined as polycentric and differentiated. With regard to platforms and online services, they are accessible through some of the most popular domestic IoT objects, such as the voice assistants Google Home or Alexa. These platforms are the target of the most comprehensive antitrust regulation in the US, the American Innovation and Choice Act, which could be considered the biggest effort in technology regulation through antitrust law since the invention of the Internet. Targeting platforms is a choice that could be understood only by considering that platforms and search engines are not only technological but especially economic and political actors.

As a contrast to platform regulation, both the AI and the IoT are not regulated through competition law, but through administrative law. The GOOD AI Act of 2021 concerns only AI applied by government services, although the definition of Artificial Intelligent system in the GOOD AI act is interesting to compare with the definition of AI in the EU AI[1033]. In fact, the former categorically excludes IoT or connected devices, whereas for the EU things are less defined. In fact, in the EU context, even IoT applications may be considered as governed

[1028] White &Case, May 27, 2019, Accessed 31 January 2023, https://www.whitecase.com/insight-our-thinking/connected-devices-challenges-both-technology-providers-and-consumers .
[1029] [1029] White &Case, May 27, 2019, Accessed 31 January 2023, https://www.whitecase.com/insight-our-thinking/connected-devices-challenges-both-technology-providers-and-consumers.
[1030] White &Case, May 27, 2019, Accessed 31 January 2023, https://www.whitecase.com/insight-our-thinking/connected-devices-challenges-both-technology-providers-and-consumers .
[1031] White &Case, May 27, 2019, Accessed 31 January 2023, https://www.whitecase.com/insight-our-thinking/connected-devices-challenges-both-technology-providers-and-consumers .
[1032]White &Case, May 27, 2019, aAccessed 31 January 2023, https://www.whitecase.com/insight-our-thinking/connected-devices-challenges-both-technology-providers-and-consumers .
[1033] According to Article 3(1) of the proposed AI Act, an AI system " […]
means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with; […]".

by the future AI act if they use algorithms included in Annex I[1034] of the proposed regulation, and especially if the application for which they are used are considered high risk[1035].

Finally, with reference to IoT regulation, there are differences between federal and national level. At a federal level, Congress delegated *en masse* the safety and compliance duties to create safe IoT objects to NIST. The Internet of Things Cybersecurity Improvement Act of 2020 defines the IoT device as having certain kind of components and using certain technology, but the main characteristics are that it uses "*transducers*" and "*can function on their own*". This characteristic may have been inspired by the California bill of 2018 concerning IoT and privacy which provides a loose definition of connected devices, only mentioning Bluetooth and Wi-Fi technology. Nevertheless, even this last bill which originates from the state that is home to Silicon Valley, a state that has consistently been socially progressive while allowing big tech corporations to flourish, did not give any action for possible complainants to challenge the low level of security that should be respected by IoT manufacturers. However, in subsection 3.1, I will demonstrate that the FTC might be the only influential but indirect regulator of all the things IoT at the federal level.

2.3. The home IoT and American legal scholarship

At this point, it is clear how the products liability theories have evolved and what the place of the IoT is in US regulatory affairs. Unfortunately, apart from Professors Elvy[1036] and Crootof [1037], barely any American legal scholar mentions the IoT as an autonomous legal and technological category in their essays and scholarly works[1038].

[1034] The kinds of algorithms considered AI are that are following "
(a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;
Logic- and knowledge-based approaches, including knowledge representation,
(b)inductive (logic) programming, knowledge bases, inference and deductive engines,
(symbolic) reasoning and expert systems;
(c)Statistical approaches, Bayesian estimation, search and optimization methods." Annex I, proposed AI Act.

[1035] According to Article 6 proposed AI act, an AI system is high risk if both these conditions are fulfilled:
" *(a) the AI system is intended to be used as a safety component of a product, or is itself a product, covered by the Union harmonization legislation listed in Annex II;*
(b) the product whose safety component is the AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment with a view to the placing on the market or putting into service of that product pursuant to the Union harmonization legislation listed in Annex II. And also the algorithms of Annex III should be considered high risk. Some examples of functions of these high-risk systems of Annex III are biometric identification and categorisation of natural person in real time (I) and education and vocational training (II)".

[1036] Stacy-Ann Elvy, *A Commercial Law of Privacy and Security for the Internet of Things* (Cambridge: Cambridge University Press 2021). Hereinafter Stacy- Ann Elvy.

[1037] Rebecca Crootof, "The Internet of Torts: Expanding civil liability standards to address corporate remote interference," *Duke Law Journal* 69,3 (2019): 583-667. Hereinafter, Rebecca Crootof.

[1038] It could be that this situation is determined by the fact that both Elvy and Crootof also take an interest in IoT contractual and privacy issues. In fact, both of them start their respective analyses by pointing out the contractual imbalance between IoT manufacturers and IoT consumers and then shift their attention to products liability at large, thus including contractual remedies such as the UCC models of contractual

With the exception of the above-mentioned scholars, the outright majority of American legal scholarship focuses more on tort law and some observations can be made as they constitute quite a homogeneous group. As far as definitions are concerned, there are no fixed ones, but it seems that a first group of scholars preferred the term robots[1039], and a second group instead preferred the term AI[1040] as umbrella terms both for automated objects and algorithms. However, the general impression is that the terms robots and AI could be used interchangeably[1041]. What is interesting is that autonomous or connected cars are considered to be the preferred use case, either to demonstrate how the current system of tort law is unfit[1042] or fit for the technological advancement also created by the IoT[1043]. Only once have I found mention of a "robot" for medical use, the Therac-25, which I will describe better in the IoT case law part of the chapter dedicated to domestic IoT medical devices[1044].

If we draw a comparison with the EU, there are more evident and frequent mentions of IoT technology and other synonyms, such as smart objects.

warranties. In particular, in her book, Professor Elvy gives a 360° evaluation of the consumer IoT, by considering cybersecurity and privacy aspects in addition to contractual and products liability issues, as her goal is to set a common commercial law of privacy for these objects. Her main conclusion is that the legal fields analysed suffer from structural deficiencies and they cannot be applied fully to damages caused by the IoT. Nevertheless, she devotes part of her book's operative chapter to updating products liability rules. Her main point is that legal scholars and practitioners could avoid quite a lot of problems concerning access to remedies under products liability law if they considered a product in a "functional" way. This means that a product does not only mean "good" but, at some conditions, also "good plus software". Moreover, she considers a functional approach to defects that should be connected to a new way of thinking about warrantee breaches. In particular, it might be necessary to create maintenance or functional defects as this would also consider problems connected to services and software. (Stacy- Ann Elvy, 316-318) Crootof, instead, claims that both contract and tort law work to shield companies from liability. Therefore, the solution should be to expand corporate liability through contract and tort measures. In particular, as far as tort measure are concerned, Crootoff suggests creating relational duties that companies should respect, the first of which should be a right to a reasonable interference through the smart object, and correspondingly, there should also be inference defects; secondly she suggests creating "IoT Fiduciaries" meaning that duties for corporation should be found in the feelings of trust that consumers have for the objects they purchase[1038]. Finally, Crootof suggests also changing the concept of causation, by extending the concept of proximate cause[1038]. Rebecca Crootof, 649-659.

[1039] See Ryan Calo, "Robotics and the Lessons for Cyberlaw," California Law Review 103,3(2015): 513; Jack Balkin, "The Path of Robotics Law," *California Law Review* 6 (2015):45-60, Ryan Abbott, "The Reasonable Computer" *George Washington Law Review* 86,1 (2018):1-45.

[1040] Anat Lior, "The AI Accident Network: Artificial Intelligence Liability Meets Network Theory," Tulane Law Review 95, 2020, Available at SSRN: 1-58, Accessed 31 January 2023, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3561948 ; Karni Chagal-Feferkorn," AM I AN ALGORITHM OR A PRODUCT? WHEN PRODUCTS LIABILITY SHOULD APPLY TO ALGORITHMIC DECISION-MAKERS," *Stanford Law & Policy Review* 30 (2019):61-114.

[1041] Such as Frank Pasquale in his book. Frank Pasquale, *New Laws of Robotics- Defending Human Expertise in the Age of AI* (Cambridge Massachusetts & London, England: the Belknap Press of Harvard University Press, 2020) or Omri Rachum-Twaig, "Whose Robot is it Anyway? Liability for Artificial Intelligence Based Robots" *University of Illinois Law Review* 4(2020): 1143-1176.

[1042] Kenneth S. Abraham and Robert L. Rabin, "Automated Vehicles and Manufacturer Responsibility for Accidents: A New Legal Regime for a New Era," *Virginia Law Review* 105,1(2019): 129-161. Mark Lemley and Bryan Casey, "Remedies for Robots", *The University of Chicago Law Review*, 2018 1311-1396.

[1043] Mark Geistfield, "A Roadmap for Autonomous Vehicles: State Tort Liability, Automobile Insurance, and Federal Safety Regulation," *California Law Review* 105(2017): 1611- 1694. Lothar Determann and Bruce Perens, "Open Cars," *Berkely Technology Law Journal* 32,2 (2017): 915-988.

[1044]Karni Chagal-Feferkorn, "AM I AN ALGORITHM OR A PRODUCT? WHEN PRODUCTS LIABILITY SHOULD APPLY TO ALGORITHMIC DECISION-MAKERS," *Stanford Law & Policy Review* 30 (2019): 88. Hereinafter Karni Chagal- Feferkorn.

Moreover, legal scholars' articles on these connected object issues have become more readily available as there are now several specialised reviews in cybersecurity and data protection[1045]. At the same time, more traditional EU private law reviews are also devoting more and more space to technological novelties[1046]. The same cannot be said when searching for the term "IoT", even when one researches it in the most relevant American reviews for legal and policy affairs. It could be that the IoT is thought of as being simply a specification of either AI or Robotics, hence it is less interesting in terms of general legal theory. Alternatively, the IoT could be viewed as a phenomenon that is more connected to cybersecurity, hence closer to regulatory matters than legal ones[1047]. It is true that in the EU, there is also a noteworthy legislative and policy incentive in IoT consumer objects legal research. In fact, it appears clear that what the dispositions imply as a "good interconnected with digital content or services", such as in the SDG, is an IoT object.

American legal scholars who mostly focus on tort and strict liability rules interpret the frictions between AI/Robotics and products liability in mainly two different ways. As a preliminary observation, hardly anyone uses products liability as a general category, but most scholars reflect on the traditional tort elements (negligence, fault, duty of care, causal link) or on strict liability premises. Hardly anyone considers contractual liability issues such as warranties and new technologies except Hubbard[1048] and the already mentioned Elvy, and Crootof.

Nevertheless, trends could be noticed and the most apparent one is that legal scholars seem to be divided into two groups. The first and smaller one comprises the (even implicitly) "technology enthusiasts" such as Abbott or Casey[1049]. Abbot, for instance, advocates new rules that take the behaviour of the machine as a standard reference, as humans are considered more likely to be responsible for errors than machines[1050]. Casey, instead, points out that the legal discourse missed an important point of the "constitution" of robots: that we could gather indirect information and observation through an inference process on the data than the object gathered.[1051]

Conversely, the second group coincides with the outright majority of scholars and has elaborated detailed legal analyses on how the AI/Robotics render the actual rules (mostly tort rules) inadequate. Most reflections are on how to evaluate fault and how to find the person who is in control, hence liable, for the

[1045] Among many, take as examples *International Data Privacy Law* and *Computer Law and Security Review*.
[1046] Among many, take as examples *Journal of European Consumer and Market Law*, and *European Review of Private Law*.
[1047] Even if there are notable exceptions such as Professor Elvy that explores all the points of frictions of the IoT with several legal fields from products liability rules, to contracts, from cybersecurity to privacy and surveillance issues.
[1048] F. Patrick Hubbard, "'Sophisticated Robots': Balancing Liability, Regulation and Innovation," *University of Florida Law Review* 66(2014): 1811-1817. Stacy-Ann Elvy, 160-195. Rebecca Crootof, 611- 622.
[1049] Bryan Casey, "Robot Ipsa Loquitur," *The Georgetown Law Journal* 108(2019): 225-286; Ryan Abbott " The Reasonable Computer," *George Washington Law Review* 86,1(2018) 1-45.
[1050] Ryan Abbot, "The reasonable computer: Disrupting the paradigm of tort liability," *George Washington Law Review* 86,1 (2018): 1.
[1051] Bryan Casey, "Robot Ipsa Loquitur," *The Georgetown Law Journal* 108(2019): 225.

AI/Robot application, what causality is and how remedies need to change. After several and similar critical parts, the more proactive and creative parts are -not surprisingly- specific to each scholar. Some scholars offer a wider recourse to strict liability. On the one hand, Abraham and Rabin suggest that, when fully autonomous cars, in which users will have no meaningful input in their functioning, become available, there should be a new Manufacturer Enterprise Liability (MER) which would create a "[…] *manufacturer financed, strict responsibility bodily injured compensation system, administered by a fund created through assessments levied on autonomous cars*"[1052]. On the other hand, Geistfield prefers to combine a regulatory approach, through the approval of federal laws concerning uniform security obligations that automated cars manufacturers should follow[1053]. In this way, tort law would just integrate federal law, and, consequently, if a manufacturer complies with federal regulations, they would be liable under strict liability in some cases only (such as a malfunctioning of the operating system due to a programming error) or negligence (e.g., if consumers and bystanders are treated differently and if the manufacturer does not respect federal law)[1054]. Other scholars, focus on the meaning of remedies and what needs to be changed to make the system work better[1055].

In the group of scholars who focus more on tort and strict liability, I personally feel that the more interesting approaches are the ones by Choi, Chagal-Feferkorn and Lior, because of the creativity of their research and approach. They try to re-think traditional tort theory and adapt it to a new context (Choi); they draft a theoretical methodology to assess legal consequences of AI-induced events (Chagal-Feferkorn); they create a multidisciplinary approach that combines legal theory and network theory (Lior). Choi's work differs in reference to the object of his analysis. He does not focus on AI or on robots, but on their fundamental unit: software, or code. Choi suggests changing a '60s legal theory, the crashworthiness theory, originally devised for cars[1056], and making it more suitable to code/software. Cars are in principle thought to crash at some point, and this is also the case for code. Software can crash not only because of negligence but also because of its structural features[1057]. In the case of software, there are no physical collisions, as in the application of the theory to cars, but the former is digital because its origin is in software and data that can cause damage[1058]. This damage could be to the physical integrity and the property of a person[1059]. A new reasonable fault-tolerant system is obtained by suggesting

[1052] Kenneth S. Abraham and Robert L. Rabin, "Automated Vehicles and Manufacturer Responsibility for Accidents: A New Legal Regime for a New Era," *Virginia Law Review* 105,1(2019):147
[1053] Mark Geistfield, "A Roadmap for Autonomous Vehicles: State Tort Liability, Automobile Insurance, and Federal Safety Regulation," *California Law Review* 105(2017): 1632-1691. Hereinafter Mark Geistfield.
[1054] Mark Geistfield, 1632-1691.
[1055] Marc Lemley, Byan Casey, "Remedies for Robots," *The University of Chicago Law Review* (2018):1311-1396.
[1056] Choi in particular cites the case *Larsen v. General Motors Corp*. as the seminal case stating that it was "statistically inevitable" for cars to crash. However, the car manufacturer owed the victim "the duty to minimise the injurious effects of such eventualities" Bryan H. Choi, "Crashworthy Code," *Washington Law Review* 94(2019):88. Hereinafter Bryan H. Choi.
[1057] Bryan H. Choi, 86.
[1058] Bryan H. Choi, 100.
[1058] Bryan H. Choi, 100.
[1059] Bryan H. Choi, 100.

combatting software redundancy with data diversity and design, including adjudication methods such as acceptance tests or voting algorithms once a discrepancy is detected and giving the software the possibility of choosing a recovery method for the error, [1060]. Also, Lior combines tort theory and IT theory to create a new methodology to assess liability with AI-based accidents. Lior combines Fletcher's non reciprocal paradigm[1061] and network theory, which is best known for its applications in creating AI neural networks but that, originally, is the study of symmetric and asymmetric relations between connected items[1062]. Through this innovative approach, Lior is able to assess liability in four technology-induced (but quite different from each other) scenarios: the spread of fake news by bots; high frequency trading algorithms (HFT) denial of service attacks (DDoS) and hiring algorithms[1063]. Finally, to assess whether traditional products liability frameworks should continue to be applied to the new way of autonomous decision-making objects[1064] Chagall-Feferkorn creates a new method that is based on an autonomy-level classification that is applied to what she calls a "thinking algorithm"[1065].

Overall, the majority of US legal scholarship has wide and flexible definitions of technological phenomena which do not require the label of IoT. This situation could be considered partly similar to the observations made about the concept of products liability. AI, Robots and IoT might be structurally different technologies, as tort, contract and strict liability are different sets of legal rules and principles. However, one can consider the latter ones as part of the products liability category, as one can use either AI or Robotics to indicate interchangeably AI, Robotics and the IoT.

3. Case law on consumer IoT devices in the US

In sub-section 2.2. it was explained why the US has always been reluctant to regulate technology through laws and regulations (although one may also see judicial cases as a form of ex post regulation) and it may only start to do so when there are economic and political issues directly connected to it, such as in the case of platforms. But what about the IoT? According to some scholars, if we think of the IoT as the most advanced branch of robotics, it could be the most transformative technology so far due toits characteristics of embodiment, emergence and social valence[1066]. What is undisputed is that, especially as far as home devices are concerned, the IoT are colonising American households at

[1060] Bryan H. Choi, 110.
[1061] "Which means that a victim has a right to recover for injuries caused by a risk greater in degree and different in order from those created by the victim and imposed on the defendant" Anat Lior 2
[1062]Anat Lior, "The AI Accident Network: Artificial Intelligence Liability Meets Network Theory," Tulane Law Review 95, 2020: 4. Hereinafter Anat Lior.
[1063] Anat Lior, 46.
[1064] Karni Chagal-Feferkorn, 65.
[1065] Karni Chagal-Feferkorn, 107-109.
[1066] Ryan Calo, "Robotics and the Lessons of Cyberlaw," *California Law Review* 103, 3(2015):515-532.

a fast pace[1067]. While the choice of purchasing an IoT device is currently just a personal choice, it may not be so for long[1068]. However, regulation at large and legal scholars tend to avoid looking at this technology singularly. Instead, courts and the FTC have already started experiencing a first wave of cases involving objects that are domestic IoT objects.

What I expected while researching the growing body of national cases on domestic IoT objects was to find negligence actions, and, in particular, the use of the Restatement Third of Torts (especially the defective design claim). Or, alternatively, I hoped to find references to the express or implied merchantability doctrines as they can now be found in the UCC. I thought I might perhaps report strict liability claims, as I had concluded at the end of subparagraph 2.1.4. on the actual evolution of product liability theories. Instead, I found that the cases concerning domestic IoTs that were brought to court (or were investigated by the FTC) mostly focused on claims concerning data privacy and data security laws, together or not with the previously cited theories. The common thread is that the object was not functioning as it should have. Hence, it was defective.

As data privacy is a branch of consumer policy that is only subject to sectorial regulations, unlike in Europe, a consistent part of the cases were actually administrative procedures before the FTC[1069]. This is because Congress has tasked it with solving unfair practices in data privacy policies towards consumers and misrepresentation[1070].

Because of the sectorial regime concerning data privacy involved in these cases, not only state laws on frauds and unfair competition were cited, but also federal law, such as the Children Online Privacy Protection Act (COPPA)[1071] or the Medical Devices Amendments act of 1976[1072], which I will discuss in subparagraphs 3.2 and 3.3 respectively. In some cases, there were also issues of pre-emption between federal law and state law[1073].

In the following pages I have divided the relevant cases according to their function, such as security devices for 3.1, or on the group of objects at large, such as connected cars in 3.4.

[1067] Stacy-Ann Elvy, "Privacy in the Internet of Things World," in *A Commercial Law of Privacy and security for the Internet of Things*, Stacy-Ann Elvy (Cambridge: Cambridge University Press, 2021), 49.
[1068] Stacy-Ann Elvy, "Privacy in the Internet of Things World," in *A Commercial Law of Privacy and security for the Internet of Things*, Stacy-Ann Elvy (Cambridge: Cambridge University Press, 2021), 25-58.
[1069] Daniel Solove and Paul M. Schwartz, *Information Privacy Law*, (Netherlands: Wolters Kluwer, Aspen Casebook series, 6th edition),786-788. Hereinafter *Solove and Schwartz*.
[1070] *Solove and Schwartz*),786-788.
[1071] "Children's Online Privacy Protection, (COPPA), 15 U.S.C. §§ 6501-6506", *Code of Federal Regulation*, https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312, Accessed 31 January 2023.
[1072] "H.R. 11124- Medical Device Amendments, Sponsor: Rogers Paul g.," Congress.gov., Accessed 31 January 2023, https://www.congress.gov/bill/94th-congress/house-bill/11124 .Hereinafter Medical Devices Amendment Act, 1976.
[1073] See below at sub-section 3.3 on Medical Devices and the IoT.

3.1. Security devices for the home

This paragraph covers cases dealt with by the FTC and the most important judicial case, *Onity*[1074].

3.1.1. FTC cases

Today, the FTC has a specific competence concerning consumer protection. Moreover, data privacy and data security are considered two subsets stemming from it. However, it was not always like this. It must be remembered that it was the US Congress that gave the FTC the task to get involved with consumer privacy issues in 1995. To protect consumers in matters of data privacy and security, the FTC applies Section 5 of FTC statute, the FTC Act[1075]. The FTC extensively interprets the concepts of "deception" and "unfairness" to sanction anti-competitive practices for consumers. In particular, a deceptive practice is about a ***material*** [1076] *"[…] representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment*"[1077]. Instead, the FTC considers as unfair a practice that "[…] *causes or is likely to cause substantial injuries to consumers themselves and it is not outweighed by countervailing benefits to consumer or competition*"[1078]. If we make the comparison, the European Commission, when acting as a competition public enforcer agent, does not have competence for data protection or cybersecurity (this is how they would loosely translate data privacy and data security) but consumer protection is one criterion to judge how anti-competitive a practice might be, and, in certain cases, whether an anti-competitive practice can be excused because of the benefits it brings to consumers[1079].

Despite this similarity, data protection public enforcement works differently in the EU. There are administrative authorities both at the national level[1080] and at the transnational level[1081] for data protection. In particular, National Data Protection Authorities (NDPAs) can fine companies for data breaches or for violation of the GDPR[1082]. It is interesting to notice that the FTC cannot (in principle) impose fines limited to the consumer data privacy and data security

[1074] See complete reference below sub-section, 3.1.2.
[1075] 15 U.S.C.A. §45 Unfair methods of competition unlawful prevention by Commission, Westlaw.
[1076] Emphasis added.
[1077] In particular, Solove and Schwartz cite as the source of this definition James C. Miller III, Chairman of FTC.
[1078] §45 (n).
[1079] Article 101(3) TFEU.
[1080] Such as the National Data Protection authorities (NDPAs) and the new CSIRTs for cybersecurity and national cybersecurity agencies
[1081] Meaning the European Data Protection Supervisor and the European Data Protection Board and ENISA, the EU cybersecurity agency.
[1082] It appears that NDPAs are quite active and in a race to fine "big tech" firms. Recently, the French NDPA Cnil fined Google because its cookies' use was not respecting the GDPR, See CNIL, "Cookies: the CNIL fines GOOGLE a total of 150 million euros and Facebook 60 million euros for non-compliance with French legislation," *CNIL*, Accessed 31 January 2023, https://www.cnil.fr/en/cookies-cnil-fines-google-total-150-million-euros-and-facebook-60-million-euros-non-compliance .

fields[1083]. It can issue fines, however, whenever companies violate the consent decree previously entered for a violation of Section 5[1084]. Furthermore, whenever the FTC has competence to regulate data security under other statutes, such as under the COPPA when minors are involved, it can impose fines as it is the primary enforcer[1085]. It can still impose non-judicial measures on companies which have violated §45, Section 5 of the FTC Act. Among the different actions, it can address injunctive remedies according to §53 of the FTC Act[1086]. Nevertheless, it is not possible for private citizens to ask the FTC for recovery: a private action for these kind of claims does not exist yet. On the contrary, in the EU, the GDPR grants private citizens the possibility to lodge a complaint with a NDPA if they allege there was a data protection violation from one company (data controller)[1087].

The FTC set of competences concerning consumer privacy protection has been judged too limited at a federal level with regard to data privacy and security applied to the IoT[1088]. Contrary to this opinion, as Solove and Hartzog pointed out, the FTC has had a tremendous role in enforcing privacy over judicial institutions. They also argue that its way of proceeding, including the forms and contents of its decisions and orders, have become a sort of Common Law of privacy[1089]. It is true that the focus of Solove and Hartzog's attention were only cases about privacy policies and how they were enforced by the FTC. Chronologically, their object of study consisted of a series of cases starting from the end of the '90s and ending at the beginning of the 2010s. Even with regard to the IoT, it is reasonable to predict that the FTC will slowly create *de facto* standards in the field of data privacy and security that will become more rule-like in nature. These standards will encompass quality standards, including the development of baseline form protections, possibly in collaboration with NIST[1090]. FTC could also extend the recognition of contributory liability for IoT domestic objects, as claimed by Solove and Hartzog with reference to privacy policies. However, for the cases that will be reported, this is still not the case.

A true problem may be that these kinds of proceedings also respond to certain choices of policy that could target some companies over other ones. Hence, they will be subject to contingent elements such as funding and what the government in charge's priorities are. In fact, the specific commission for these affairs is composed of five people nominated by the US President and confirmed by the Senate for a seven-year term[1091].

[1083] Solove and Schwartz, 846.
[1084] Solove and Schwartz, 846.
[1085] See below sub-section 3.2 "Toys and children devices".
[1086] Solove and Schwartz, 846.
[1087] Article 77 GDPR.
[1088] Stacy-Ann Elvy, "The Current privacy and Data Security Legal Landscape," in *A Commercial Law of Privacy and security for the Internet of Things*, Stacy-Ann Elvy (Cambridge: Cambridge University Press, 2021),82-83.
[1089] Daniel J. Solove and Woodrow Hartzog, "The FTC and the New Common Law of Privacy," *Columbia Law Review* 114, 3(2014):589.
[1090] See supra Chapter VI, 2.2.
[1091] Solove and Schwartz,846.

Despite the limitation of its powers regarding consumer and data protection, the FTC has been very active during recent years with more than 50 cases involving new technologies such as social media objects[1092], and now even IoT cases are growing in number. Solove and Schwartz rightly observed that during recent years, the FTC has focused more on the data security aspect more than on the data privacy one[1093].The cases below show that there is a good balance between data privacy and data security aspects in investigating home IoT object malfunctioning.

I. TRENDnet

The first case that will be commented on is the case of TRENDnet[1094], a manufacturer of surveillance systems, and in particular, smart cameras, in 2014. This case is important as it was the first one in the US to publicly concern domestic IoT objects. Specifically, it was about a set of IP cameras called "SecurView", which allowed consumers to monitor what was happening in their own home through the access of live video and audio feeds directly from the camera over the Internet[1095]. As of 2010, *TRENDnet* also implemented a feature called Direct Video Authentication Setting (DVAS), which also allowed users to turn off the option to fill in credentials (ID login and password) when they needed to access the camera audio and visual feed[1096]. In 2011, *TRENDnet* also implemented a mobile phone app for Android[1097].

The FTC decided to lodge a complaint against this manufacturer of smart cameras for several reasons. Firstly, *TRENDnet* had advertised its line of smart home video IP cameras, SecurView, as highly reliable in terms of cybersecurity[1098]. Contrary to this public image, *TRENDnet* failed to encrypt its customers' personal data (mainly their login credentials) with a software that was already available for purchase[1099]. Moreover, *TRENDnet* implemented a function with which it was possible for the user not to be asked the credentials of the smart cameras whenever they wanted to access their devices' recordings[1100]. Unfortunately, the users who had enabled the turning off of their credentials with the DVAS system had involuntarily made their IP address public[1101]. In 2012, a hacker took advantage of the failures and vulnerability of *TRENDnet* SecurView cameras and hacked more than 700 subjects, publishing links to the live feeds of

[1092] Solove and Schwartz,847.
[1093] Solove and Schwartz, 975.
[1094] "In the Matter of TRENDNet, 2014," Federal Trade Commission, Accessed 31 January 2023, https://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf .
Hereinafter *TRENDnet* Complaint.
[1095] §4 *TRENDnet* Complaint.
[1096] §6 *TRENDnet* Complaint.
[1097] §6 *TRENDnet* Complaint.
[1098] §7(b) *TRENDnet* Complaint.
[1099] §8(a) *TRENDnet* Complaint.
[1100] §6 *TRENDnet* Complaint.
[1101] §10 *TRENDnet* Complaint.

the users[1102]. This increased the risk of theft or other criminal activity for hacked consumers[1103]. That is why the complaint developed into a decision and order[1104].

Following §45 of the FTC Act, the FTC ordered *TRENDnet* to not "*misrepresent in any manner, expressly or by implication: the extent of the security of device functionality and its security, privacy, confidentiality of any info".*[1105] Moreover, it was further ordered that *TRENDnet* took all the means available to improve its security system[1106] and to obtain periodical assessments "[…] *from a qualified, objective and third party professional*".[1107] Among the many requirements composing this order (which would last 20 years from its notification[1108]) there was also the obligation for *TRENDnet* to notify the affected consumers that their camera had a flaw[1109].

II. Vizio

The second very important case was *In the Matter Vizio*[1110], in 2017. Vizio was a producer of smart televisions. Thanks to software within the television device, it was possible for *Vizio* to access all data concerning consumers' tv-watching habits, without the users' express consent. *Vizio* decided to settle the case and was meant to pay 2.2 million dollars to the FTC itself and the State of New Jersey. Moreover, a series of behavioural instructions are contained in the decision and order.

The first part of the order concerns the prohibition of misleading representation under §45 FTC Act of the covered information, which is basically the data concerning "*but not limited to (1) production registration data (2) viewing data (3) internet protocol (IP) addresses (4) User ID or other identifiers and (5) geolocalisation data*"[1111]. In the second part of the order, it is imposed that *Vizio* inform, separately from other privacy documents or terms of use, "*1) the types of Viewing Data that will be collected and used; (2) the types of Viewing Data that will be shared with third parties; (3) the identity or specific categories of third parties; and (4) all purposes for defendants' sharing such information* "[1112].

This part of the order at times resembles Article 12 and 13 GDPR, which concern the principle of transparent information for the data controller (the entity

[1102] §10 *TRENDnet* Complaint.
[1103] §13 *TRENDnet* Complaint.
[1104] "In the Matter of TRENDNet , 2014," Federal Trade Commission, Accessed 31 January 2023, https://www.ftc.gov/system/files/documents/cases/140207trendnetdo.pdf.
.Hereinafter *TRENDnet* Decision and Order.
[1105] I. A), 1) and 2) *TREND*net Decision and Order.
[1106] II, A),B),C),D),E,)F),G),H) *TREND*net Decision and Order.
[1107] III *TREND*net Decision and Order.
[1108] IX *TREND*net Decision and Order.
[1109] IV *TREND*net Decision and Order.
[1110] "In the Matter Vizio, 2017," Federal Trade Commission, Accessed 31 January 2023, https://www.ftc.gov/system/files/documents/cases/170206_vizio_stipulated_proposed_order.pdf.
Hereinafter, *Vizio* Decision and Order.
[1111] Definition A *Vizio* Decision and Order.
[1112] II. A), *Vizio* Decision and Order.

that has control over the data subject's personal data) and the information to be provided where personal data are collected by the data subject respectively.

Similarly, consent must be "affirmative and express"[1113], which is reminiscent of the Article 7 GDPR content on the criteria to follow in order to obtain legitimate consent. The order also has more concrete actions such as the deletion of the data collected up to 1st March 2016 [1114]. Lastly, *Vizio* should undergo a mandatory privacy programme. This programme is similar to all Articles in the GDPR concerning the nomination of the data controller and the data protection impact assessment (DPIA)[1115]. In the GDPR, however, the instructions are more general, whereas here they are specific to the case at hand.

Finally, as in *TRENDnet*, *Vizio* contains an order for a privacy assessment to be carried out by a third party. In the GDPR, there are certification bodies which are accredited third party bodies (such as Notified Bodies) which produce certifications[1116]. However, they cannot be used as assessment bodies by the NDPAs. The NDPAs deal solely with verifying whether the certifications are suitable or could decide to withdraw a data protection certification as a sanction to a data controller and processor[1117]. In the end, *Vizio* accepted all these conditions as part of the settlement.

III. D-Link

Another example of how §45 was used is the case involving *D-Link*, a well-known Taiwanese company with a US subsidiary. *D-Link* produced IP cameras like *TREND*net, and routers for the home. Routers are not IoT objects *per se*, but it is true that they make Wi-Fi available for all the appliances in the home, hence, they too are a sort of gateway. The complaint resulted, as in the *TRENDnet* case, in a settlement through an FTC decision and order[1118]. Much like *TRENDnet*, *D-Link* had advertised that its devices were safe. However, there were considerable vulnerabilities both in the company's routers and Internet-cameras.

Like *TRENDnet*, *D-Link* had implemented a free mobile app "mydlinkLite" to allow a specific user to access and check on both their *D-Link* IP cameras and routers. Once the login and user credentials were filled in, the user was constantly logged into the system[1119]. In the list of *D-Link* security failures, the FTC argued that this was not sufficient to protect routers and IP cameras "[…] *from widely known and foreseeable risks of unauthorized access, including by failing to protect against flaws that the Open Web Application Security Project has ranked*

[1113] II.B), *Vizio* Decision and Order.
[1114] III, *Vizio* Decision and Order.
[1115] See Articles 27 and 35 GDPR and In the Matter Vizio, Order, IV, A, B, C, D, E.
[1116] Article 42 GDPR.
[1117] Article 58(1)(c) and (2)(h).
[1118] "D-Link , Case Proceedings", *FTC website*, Accessed 31 January 2023, https://www.ftc.gov/legal-library/browse/cases-proceedings/132-3157-x170030-d-link.
[1119] § 12 of the "D-Link Complaint, Redacted Version 2018," Federal Trade Commission, Accessed 31 January 2023, https://www.ftc.gov/system/files/documents/cases/170105_d-link_complaint_and_exhibits.pdf, hereinafter *D-Link* complaint.

among the most critical and widespread web application vulnerabilities since at least 2007."[1120] What is interesting in this complaint, compared to *TREND-Net* and *VIZIO,* is that, in *D-Link*, no harm had been caused to consumers at that time. As I will show in all the other following cases, courts are generally reluctant to recognise potential harm, even when it was reasonable to expect it. It may be that the FTC protects consumers more than the courts *de facto* even if it cannot be accessed directly by them. In part, this is to be expected, as consumer protection is one of the tasks of the commission, but how will it balance these actions, especially the misrepresentation of product information with the freedom of expression and commercial speech in the First Amendment, which also protects commercial advertisement? For the moment, this is still unclear.

In the end, *D-Link* agreed to settle the complaint. As in the previous cases, it is nonetheless interesting to analyse the proposed and stipulated order to understand which kind of behaviours and actions *D-Link* was urged to implement. As the software programme used for the app was the source of the IoT's vulnerabilities, the main measure requested was to implement a comprehensive software security programme for a period of twenty years after the entry of this order. Implementation of the programme is similar to what the FTC had suggested concerning the privacy programme. In fact, *D-link* must document the content, implementation and maintenance of the security programme and the designation of a person responsible for it in writing[1121]. Point E of the order is structured in a way that, for EU data protection specialists resemble parts of Article 35(1)[1122] and (7)[1123] GDPR, specifically with regard to the obligation to draft a DPIA for a high-risk processing activity, such as the one discussed in this case, even if data security, and not data privacy, is the main focus of this complaint. Point E in fact mentions the obligation to draft a security plan by taking into account the "[…] *functionality and features that will affect the security of Covered Devices* [routers and IP cameras]"[1124]. This also includes "*performing threat modelling to identify internal and external risks to the security of data*"[1125] and many other requirements. This software security programme must be

[1120] §15 *D-Link* Complaint.
[1121] "In matter D-link, 2019," Federal Trade Commission, Accessed 31 January 2023, https://www.ftc.gov/system/files/documents/cases/dlink_proposed_order_and_judgment_7-2-19.pdf . Hereinafter, *D-Link* Decision and Order.
[1122] Article 35 (1) GDPR states that a DPIA (Data Protection Impact Assessment) is needed "[w]*here a type of processing in particular using new technologies, and taking into account the* ***nature***, ***scope***, ***context*** *and* ***purposes*** *of the processing, is likely to result in a* ***high risk*** *to the* ***rights*** *and* ***freedoms*** *of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks."* (Emphasis added)
[1123] The minimum requirements contained in Article 35 (7) GDPR for a DPIA are the following "[…]
(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and
(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned." (Emphasis added).
[1124] E(1) *D-Link* Decision and Order.
[1125] E(2) *D-Link* Decision and Order.

effectively assessed by a third party every two years.[1126] The assessor chosen to assess the software security programme must also be agreed by the FTC[1127] and must be qualified as a Certified Secure Software Lifecycle Professional (CSSLP)[1128], among many other qualifications. Finally, point IV of the order establishes that each year, a senior corporate manager must provide the Commission with certification that "[…] (*1) the requirements of this order have been established, implemented and maintained and (2) Defendant is not aware of any material noncompliance that has not been (a) corrected or (b) disclosed to the Commission*" [1129].

One of the main differences between the EU data protection rules and the US consumer protection remedies is that the FTC security software programme instructions do not take into account the many references to freedoms and fundamental rights the EU GDPR does, especially with reference with the EU DPIA. This is actually a consequence of a different constitutional value that is placed on data protection/ data privacy by the EU and the US respectively. In fact the EU has data protection as an individual and separate right[1130], even in relation to privacy. In the US, there is no perfect equivalent for data protection, but data privacy and data security are part of the much larger consumer protection policy. However different, these two different legal concepts serve the same effect in practice. In the place of fundamental rights the FTC uses the clauses of protecting the consumer from a significant risk of harm. In the complaint, the FTC explained that "[b]*y creating these vulnerabilities, Defendants put consumers at a significant risk of harm in a variety of ways.* […] *For example, using a compromised router, an attacker could re-direct consumers seeking a legitimate financial site to a spoofed website, where they would unwittingly provide the attacker with sensitive financial information […] Similarly, by exploiting the vulnerabilities described* […], *an attacker could compromise a consumer's IP camera, thereby monitoring consumers' whereabouts to target them for theft or other criminal activity"*[1131]. In a way, the FTC partly exercises the functions of what in the EU is an NDPA (national data protection authority)[1132] except that it does not have the specific power in this case to issue fines. However, non-compliance with alternative judicial measures such as this one can have serious consequences, as companies that violate the settlement could be liable to up to 16,000$ for each violation, and injunctive or other equitable relief is available[1133].

IV. Tapplock

[1126] II *D-Link* Decision and Order.
[1127] II B *D-Link* Decision and Order.
[1128] II A *D-Link* Decision and Order.
[1129] IV A *D-Link* Decision and Order.
[1130] See Chapter III part on Data Law,2.1.
[1131] §18 *D-Link* Complaint.
[1132] See Article 58(d) GDPR that each national data protection authority has, among its corrective powers, "to order the controller or processor to bring processing operations into compliance [with the GDPR], where appropriate, in a specified manner".
[1133] Solove and Schwartz , 847.

The last case that is still pending but that promises to be extremely interesting is *Tapplock*[1134]. *Tapplock* is a Canadian company which produces smart locks. Interestingly enough, this is the first of the cases cited that mentions smart locks as IoT objects[1135]. *Tapplock* advertised that it produced smart locks that were "*Bold. Sturdy. Secure*."[1136], and designed with "*anti-shim and anti-pry technology*"[1137]. However, despite these and other claims, such as the one to possibly share the smart lock key with others and then also revoke it[1138], these objects were not safe. The complaint goes into detail enumerating the several cybersecurity liabilities of these objects such as the fact that *Tapplock* API allowed "[…] *researchers to bypass the authentication process in order to gain full access to the accounts of all Tapplock users and their personal information*"[1139]. Moreover, researchers also demonstrated that it was also possible to open and lock the door even without having the credentials and that it was not possible to revoke access to the smart lock once the user had given this authorisation to another person[1140]. All these claims constituted a "*deceptive representation regarding security*"[1141] and also a "*deceptive representation regarding protection of personal information*"[1142], thus infringing §45, Section 5 of the FTC Act.

The subsequent decision and order is actually not so different from the measures taken in *D-Link*. For example, the II order is a quite detailed Mandated Device Security and Information Security Programme[1143] (which sums up the two privacy and security programmes of *Vizio* and *D-Link* respectively) along with the prohibition against misrepresentations about privacy and security[1144]. Moreover, *Tapplock* would be obligated to undergo a device and information security assessment by a third party[1145], to cooperate with a Third Party Information Security Assessor[1146] , as in D-Link, and an annual certification obligation that the order is respected[1147]. Lastly,, there is a set of more procedural requirements, such as for *Tapplock* to acknowledge the order[1148], and to make periodic submissions of compliance reports and notices[1149] to the FTC commission about the implementation of the order and, for a period of 20 years after issuance of the order, *Tapplock* will be obliged to keep specific kinds of records and to retain

---

[1134] "In the Matter of Tapplock, Inc., 2020," Federal Trade Commission, Accessed 31 January 2023, https://www.ftc.gov/system/files/documents/cases/1923011c4718tapplockorder.pdf, hereinafter *Tapplock* Decision and Order.
[1135] §3 Accessed "In the Matter of Tapplock, Inc., 2020," Federal Trade Commission, Accessed 31 January 2023, https://www.ftc.gov/system/files/documents/cases/1923011c4718tapplockcomplaint.pdf, hereinafter *Tapplock* complaint.
[1136] § 8 *Tapplock* complaint.
[1137] § 9 *Tapplock* complaint.
[1138] §11 *Tapplock* complaint.
[1139] §14(a) *Tapplock* complaint.
[1140] §14 (a),(b) *Tapplock* complaint.
[1141] §§ 17-18 (Count I)Tapplock complaint.
[1142] §§19-20 (Count II) Tapplock complaint.
[1143] II. *Tapplock* Decision and Order.
[1144] I. *Tapplock* Decision and Order.
[1145] III. *Tapplock* Decision and Order.
[1146] IV *Tapplock* Decision and Order.
[1147] V *Tapplock* Decision and Order.
[1148] VI *Tapplock* Decision and Order.
[1149] VII *Tapplock* Decision and Order.

them for five years[1150]. Finally, *Tapplock* will have an obligation of compliance monitoring[1151].

This order is also different because, for the first time, not only does it integrate the word IoT in its text, but it also prescribes orders and injunctive remedies not even alleging the potential harm on consumer, as in D-Link, but because an FTC bureau researcher conducted an investigation about it.

V. Comparison with EU law

How would these cases be solved in the EU? In the EU, these cases could have been challenged through national contractual or tort remedies covering products liability issues not covered by the PLD, depending on the value of these objects and the monetary entity of damage quantified by the courts. Ultimately, some consumers might also start the product recall process because it was not sufficiently safe through the RAPEX system (see Chapter III). Moreover, they may have lodged complaints before their NDPAs if their legal system did not allow them to bring product liability and data protection claims together. It must be noted that the PLD could have applied but with some *caveats*.

As far as the actual PLD is concerned, the IP cameras would have not been considered secure according to Article 6 PLD. The damage, according to Article 9, could have been considered under the economic aspect (letter b) if, for instance, one consumer had experienced theft because of the defectiveness of the product and if the value of the things stolen was up to or more than 500 euros. Hypothetically, according to letter 9 a) PLD, damages consisting in personal injuries could have a wide application according to the reasoning of AG Bot in *Bostonmedizintechnik* and could even be applied in the absence of personal injury, such as in the *D-Link* case. However, in *Bostonmedizintechnik,* the objects causing harm (actual or potential) were implanted medical devices with an inherent higher risk for human health than all the security objects cited above. In the event that immaterial damage had occurred, the PLD principles would most likely need to be integrated with national laws. In this case, immaterial damage could be a state of fear and anxiety of being attacked, whether the data breach had taken place or not. Depending on the procedural law of the state, the *Henning Veedfald* jurisprudence should allow a recovery of immaterial damages concurrently with the physical and economic ones. However, there are huge discrepancies in recognising this kind of damage throughout the 27 MS, hence the results of these hypothetical actions might considerably differ from state to state.

3.1.2. Judicial case: Onity

[1150] VIII *Tapplock* Decision and Order.
[1151] IX *Tapplock* Decision and Order.

A judicial case concerning security and surveillance of the home (although mostly related to hotels) is the *US Hotel Resort Management et al v. Onity*[1152]. *Onity* was a producer of smart locks for businesses, especially hotels[1153]. Its locks were considered safe until a software engineer from Mozilla demonstrated that these locks were easily hackable by using less than $50 worth of materia[1154]l. The video went viral on YouTube and the hotel owners who had purchased *Onity* smart locks asked *Onity* to do something to fix this situation[1155].

Onity suggested either the hotel owners put a metallic cap on the lock in order to avoid hacking or, as an alternative, to completely refit the locking system at their expense[1156]. The hotel owners deemed these two proposals to be unacceptable and the hotel owners sued *Onity* through a class action lawsuit, by claiming that the product sold was manifestly defective and even if there had not yet been an injury/damage, it was almost certain that the being hacked was an impending possibility given the 'viral' state of the video[1157]. The plaintiffs' claim framed this case as products liability litigation, as several producst liability theories summarised in 1.1 were employed by the plaintiffs. Firstly, they asserted a claim for breach of express warranty; secondly, a claim for breach of an implied warranty of merchantability. Thirdly they asserted a claim under the Magnuson Moss Warranty act[1158] and a claim for unjust enrichment[1159].

However, in this case, the judge did not order the manufacturer *Onity* to pay for poor cybersecurity, instead the action was stopped for lack of standing. Judge Richard Nelson granted the motion filed by *Onity* to dismiss the case with prejudice to the plaintiffs as they lacked standing, by relying on the US Supreme Court precedent *Clapper v. Amnesty International*[1160]. According to *Clapper*, in order to satisfy the conditions of the federal code of procedure Article III the injury must be "*[1] concrete, particularized, actual or imminent, [2] fairly traceable to the challenged action and [3] redressable by a favourable ruling"*[1161]. According to the Judge, in the *Onity* case, the injury was not impending, and were it the case "*it would only be the result of a third party intruder's decision to gain access via*

[1152] U.S. Hotel and Resort Management, Inc., et al.,v. Onity, Inc. United States District Court-District of Minnesota, Civil No. 13-1499 (SRN/FLN), 2014, Accessed 31 January 2023 https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1818&context=historical. hereinafter *Onity*.
[1153] *Onity* 1-3.
[1154] *Onity* 1-3.
[1155] *Onity* 1-3.
[1156] *Onity* 1-3.
[1157] *Onity* 1-3.
[1158] The Magnuson-Moss Warranty Act is a federal statute of 1975 which concerns warranties on consumer products. Specifically, the law does not require a product to have a warranty, but if it does, then the warranty must comply with this law. This law was enacted because of the rising habit of using warranties or disclaimers in an unfair or misleading manner. "Magnuson-Moss Warranty Act", Wikipedia, Access 31October 2022, https://en.wikipedia.org/wiki/Magnuson%E2%80%93Moss_Warranty_Act. Moreover, according to the new Magnuson Moss Warranty FTC improvements act, the FTC is authorised to develop regulation on written warranties. "Magnuson Moss Warranty- Federal Trade Commission Improvements Act," Federal Trade Commission, Accessed 31 January 2023, https://www.ftc.gov/legal-library/browse/statutes/magnuson-moss-warranty-federal-trade-commission-improvements-act.
[1159] Onity, 3.
[1160] "Clapper v. Amnesty International USA, 838 F. 3d 118,(2013)" Legal Information Institute, Accessed 31 January 2023, https://www.law.cornell.edu/supremecourt/text/11-1025. Hereinafter *Clapper.*
[1161] Clapper v. Amnesty International as cited at p.5 *Onity.*

the publicized means"[1162]. What is interesting is that the judge made several comments about the choice of judgments that plaintiffs used as reference to make their case.

Judge Richard Nelson first criticised the choice of the "no injury" doctrine argument by the plaintiffs[1163]. The fact that the locks were still functioning even when the complaint was filed made it unlikely that the damage was "impending" in order to be granted standing[1164]. Citing *Clapper* again, the judge stated that the further costs sustained by the complainants were the product of their fear of future intrusion and theft[1165]. Thus, these costs did not satisfy the standard of imminence that is required for a claim to have standing[1166]. It must be noted that *Clapper* as a constitutional precedent was passed with a slight majority within the same Supreme Court[1167]. *Clapper* concerned the Foreign Intelligence Surveillance Act (FISA) and how it could infringe constitutional rights and had a huge effect on all data privacy and security cases included *Onity* [1168].

The same principles of *Clapper* would also be repeated and strictly applied in *Spokeo*[1169] two years after *Clapper*. In *Spokeo*, the plaintiff Mr Robins had been incorrectly identified and was described as something he was not by Spokeo, a "people search engine" which future employers use. Despite not being a general allegation of damage as in *Clapper*, the Court considered that Mr Robins did not suffer concrete damage, as concrete is synonymous of tangible. In the majority of the Court's opinion, Congress was "[…] *charged with elevating and recognising intangible harms through statutory law.* […] *However, even in the case of a statute breach giving a right to the plaintiff*, […] *the plaintiff would need to prove also the damage in fact*[1170]". Hence, the court considered that by the proceedings' documents, Mr Robins had not demonstrated his legal standing. This time only Justice Ginsburg and Sotomayor dissented. Justice Ginsburg explained that Mr Robins did not seek redress "[…] *for Spokeo's spread of misinformation about him and this would impact concretely his capability to find a job, for instance*"[1171]. It would seem that *Onity* is in between the path started by *Clapper* and continued with *Spokeo*.

Interestingly enough, the plaintiffs had built their case by relying on products liability cases arising from the 8th circuit, among which the famous *Brihel v. General Motors Corp*.[1172], which was about a car's defective ABS system, and several decisions from Minnesota[1173]. Also according to a EU standard, this could

[1162] *Onity* 6.
[1163] *Onity* 6-9.
[1164] *Onity* 6-9.
[1165] *Onity* 6-9.
[1166] *Onity* 6-9.
[1167] It was a 5-4 majority. Justice Alito delivered the opinion. Justice Breyer delivered the dissenting opinion joined by Justice Ginsburg, Justice Sotomayor, Justice Kagan. Solove and Schwartz, 807.
[1168] Solove and Schwartz, 807.
[1169] Spokeo, INC. v. Robins, 136 S.Ct.1540 (2016), hereinafter, *Spokeo*.
[1170] *Spokeo* judgment reported by Solove and Schwartz, 810.
[1171] *Spokeo* judgment reported by Solove and Schwartz, 811.
[1172] Brihel v. General Motors Corp., 172 F.3d 623 (8th Cir. 1999) cited by Judge Nelson in *Onity*.
[1173] *Onity* n. 3, 13.

be seen as a product liability case based on the concept of defectiveness and safety and how to calculate potential pecuniary damage[1174]. Instead, the Judge adopted a formal approach and framed the main issue as concerning standing. Despite this, the Judge had to motivate why the products liability cases were not relevant for them[1175]. According to the Judge, the plaintiffs were not right in citing the case *Zurn Pex Plumming*[1176] because both the products and facts could not be compared: *Zurn Pex* was about a plumbing system that was about to fail within the warranty period. Therefore, no need of "external damage" to have standing[1177].

More importantly, according to the Judge in *Onity*, the plaintiffs had never demonstrated that the locks had stopped working normally because of their alleged cybersecurity vulnerability[1178]. It is interesting to point out that the Court does not dismiss all the product liability cases cited by the plaintiffs alone, but suggests that a better analogy to the present case are the so-called "lost data" cases[1179] such as *Reilly v. Ceridian Corp*[1180] and *Accord Galaria v. Nationwide Mut. Ins. Co*[1181]. In particular, in *Reilly,* the plaintiff failed to demonstrate that there had been a misuse of their personal information after a data breach; in *Accord Galaria* there was no standing for the plaintiff, even though the personal information stolen was actually misused. In the case at hand, the plaintiff's personal information held in an insurance company computer had been shared. As far as the lost data cases are concerned, *"[…] courts have split somewhat on the question of standing*"[1182]. The judge probably refers to cases such as *Resnick v. AVMed*,[1183] a case which concerned a data breach of medical, health and other general personal data (according to the GDPR). In *Resnick*, the plaintiffs proved their standing by demonstrating that before the data breach they had never been subjected to identity theft. Conversely, they did experience identity theft after the data leak. Nevertheless, the *Onity* judge argues that already from *Reilly* and *Accord Galaria*, there had been a consensus on the degree of impendency that the data breach needed to have in order to consider whether there was standing or not[1184]. The principles used in the data cases are actually the same as *Clapper* even when the judgment's date was prior to the US supreme court precedent.

I find *Onity* to be a particularly interesting judgment as here the Court indirectly explained not only how to apply a US supreme court precedent on standing and rules of procedure, such as *Clapper*, but also on how to construct a

[1174] See Chapter V.
[1175] *Onity* n.3 p. 13.
[1176] In reZurn Pex Plumbing Products liability Lit. 644 F.3d 604 (8th Cir. 2011),as cited by Judge Nelson in *Onity,* hereinafter Zurn Pex.
[1177] *Onity* p. 13-16
[1178] *Onity* p. 14-16.
[1179] *Onity* p. 9.
[1180] Reilly v. Ceridian Corp., 664 F.3d 38, 43 (3rd Cir. 2011), hereinafter *Reilly*. Cited by Judge Nelson in *Onity*.
[1181] Accord Galaria v. Nationwide Mut. Ins. Co. F. Supp. 2d, 2014 WL 689703, *5, *7 (S.D. Ohio Feb. 10, 2014), hereinafter *Accord Galaria*. As cited by Judge Nelson in *Onity*
[1182] Onity p.11.
[1183] Resnick v. AvMed, 693 F.3d 1317 (11th Cit. 2012), as cited by Justice Nelson in *Onity* hereinafter *Resnick.*
[1184] *Onity* p.11-13

case involving a technological defect. The judge argued that the product liability cases needed to be better selected and, with reference to harm caused by data breach, which elements needed to be proved in order to have *locus standi*. This could also mean that if the future plaintiffs follow the indications of the Court, they would have better chances to win the case.

The main difficulty for the plaintiffs in *Onity* is that they relied on products liability cases and it was objectively difficult to create analogies with more traditional objects, as smart locks are IoT and data security and data privacy almost always add on to other claims. That is why *Onity* does not present the three main kinds of claims that are common in US data breach cases, which are claims of emotional distress, increased risk of future harm or expenditures to reduce the risk of harm.[1185] Nevertheless, I argue that the analogy of the judge with the data breaches cases is incorrect: all the judgments cited concerned personal information (personal data) which had or had not been later misused. In this case, there was no personal information to rely on: if we look at the functioning of this very simple smart lock (which was an elementary model for hotels) what this smart lock had was just a more or less random combination of codes that opens a door. The only personal information that could have been hacked is a person's telephone number, or the ID of the device. What is precious and private are the belongings of the person that is staying in the hotel room and that was what the claimants had in mind when thinking about future legal action against them.

Besides, despite *Clapper*'s procedural interpretation of the requirement of the injury-in-fact, which is justified to not overflow courts with petty litigations, it is difficult to argue that a smart lock that had a verified cybersecurity defect would not be compromised in the future while continuing to be defective nonetheless. It is quite a simple object, maybe less refined than the IP cameras in the *TRENDnet* or *D-Link* cases, and it is even less refined than the "unbreakable" *Tapplock* smart locks. However, these locks have one function: to maintain the security of the environment that they are supposed to either monitor or to lock. Especially for the lock, if this vulnerability exists, I think that the impendency and immediacy requirements could be easily satisfied.

One other way through which the plaintiff could have tried to win the case was through the implied merchantability warranty, as will be shown in the following *Vtech* case (*infra* in Toys and Children's Devices subparagraph).

It is important to know that there was probably already a thief at the time of the proceedings who was robbing the hotels by exploiting the demonstration video of how the key was hackable, but this was unknown by the hotel owners at the time of the judgment[1186]. I expect that if the news relating to the thief had been

[1185] Solove and Schwartz, 960.
[1186] Thimothy Geigner, " The Epic Crime Spree Unleashed by Onity's Ambivalence To Its Easily Hacked Hotel Locks," *techdirt*, 1 September 2017, Accessed 31 January 2023, https://www.techdirt.com/2017/09/01/epic-crime-spree-unleashed-onitys-ambivalence-to-easily-hacked-hotel-locks/.

public by the time of the judgment, the legal reasoning may have been different. Certainly, the imminence and impending theft requirements would have been satisfied knowing that a thief had already been caught exploiting that specific vulnerability. However, it appears that the requirements concerning standing introduced by the *Clapper* judgment will continue to be applied strictly by US courts as a prerequisite for evaluating damage by new technologies, whereas the FTC will use consumer protection as leverage for cases where consumers have or have not yet experienced damage, such as in *D-Link* and in *Tapplock* cases.

I. Comparison with EU law

How would this case be judged by the CJEU? Surely, as a product liability case if the plaintiff had demonstrated that the damage was over 500 euros. An entire defective smart lock system in a hotel can easily surpass this threshold of Article 9 b). The video on Youtube would have been proof of the product's defect and that the object did not meet the expected safety requirements according to Articles 4 and 6 PLD. However, it is true that the PLD does not state anything concerning future pecuniary damage. Most probably, the CJEU would have left compensation for this kind of damage to the laws of the referring country, provided that they delivered a solution in harmony with the EU principles of equivalence and effectiveness as was the case in *Elisabeth Schmitt* concerning liability of the NB[1187]. Probably, jurisdictions such as Italy would reject the claims unless proof of effective damage is satisfied.[1188]

Nevertheless, it must be said that it is an incomplete comparison: in the EU, the CJEU has not yet pronounced on any case concerning an IoT[1189]. However, it is also likely that EU future product liability cases concerning new technologies might involve cybersecurity issues as product defects. What is to be expected is that in future, product liability claims will almost always be connected to data protection and data security, whenever they involve an IoT home object.

3.2. Toys and children's devices

Connected, smart, or IoT toys, whatever name we choose, are a booming market: Juniper research estimated its worth at around $18 billion by 2023[1190]. Interestingly enough, they are the kind of IoT devices that, more than others, have started to become part of the literary imagery. One may think of Kentuki toys, furry plush connected toys that allow "owners" to spy and be spied consensually, as in the dystopian novel *Kentuki* by Samantha Schweblin[1191]. Or, maybe, one can recall the sensitive educational robot and children's companion who is the

[1187] See references in Chapter II.
[1188] See discussion Article 9 PLD in Chapter V.
[1189] At the moment of writing, meaning 13 August 2022.
[1190] Sharon Shasha, Moustafa Mahmoud, Mohammad Mannan, and Amr Youssef, "Playing With Danger: A Taxonomy and Evaluation of Threats to Smart Toys," *IEEE Internet of Things Journal* 6, 2(2019): 2986.
[1191] Samantha Schweblin, *Kentuki*, (Rome: SUR,2019. Italian translation from Spanish).

protagonist in Kazuo Ishiguro's *Klara and the Sun*[1192]. Despite this, scholars have been warning for a long time about how these toys had cybersecurity risks, such as hacking of data or constant surveillance by cyber-criminals. These cybersecurity failures can have even worse psychological effects when the user is a child, who can truly love a smart-toy as a best friend and be influenced by what the smart-toy tells him or her to do[1193]. These two cases are representative of the kind of legal claims parents whose children owned a smart toy tried to bring to court.

3.2.1. VTech Data Breach Litigation

In *VTech Data Breach litigation*[1194], there are several interesting issues: the first one concerned whether to consider the data breach of the interactive toys produced by *VTech* and subsequently hacked, as a breach of contract (counts I-II). The second issue was whether a low level of cybersecurity also involved the breach of the implied warranty of merchantability (counts III-IV). Thirdly, it was interesting to observe that there was also a count of unjust enrichment as in the previous case *Onity*. This count in particular follows the violation of the Illinois consumer fraud law but is less connected to the purpose of this research, therefore I will mention it only in a cursory way.

Briefly, the facts are as follows. *VTech*'s toys main difference with traditional toys is that they are interactive and connected to two learning platforms. Basically, they are IoTs for children. These toys had to be activated by parents entering their personal data (personal information in American Privacy parlance) such as email, name, surname and debit card details and then proceeding to create an account for their child[1195]. In 2015, a hacker, who was later arrested, managed to get into the *Vtech* system and was able to retrieve all the personal data of both parents and children, including messages exchanged by the children[1196]. A group of parents decided to bring a class action lawsuit against *VTech*.

The first part of the judgment is of great interest for IoT products liability theories application in the US. The true issue was that the toys turned out to be defective, even if this adjective is never employed throughout the memorandum and order. If we look at this case from a European legal scholar point of view, this case would have required the application of either the RAPEX security recall system, or, if damage consisted of personal injuries or property damages of more

---

[1192] Kazuo Ishiguro, *Klara and the Sun*, (London: Faber&Faber, 2021).
[1193] Sharon Shasha, Moustafa Mahmoud, Mohammad Mannan, and Amr Youssef, "Playing With Danger: A Taxonomy and Evaluation of Threats to Smart Toys," *IEEE Internet of Things Journal* 6, 2(2019): 2986.
[1194] "United States Distrct Court For the Northern District of Illinois Eastern Division *IN RE VTECH DATA BREACH LITIGATION No 15 CV 10889, No15 CV 10891, No15 CV 11620, and No15 CV 11885*,(2016)" Casetext, Accessed 31 January 2023, Accessed 31 January 2023, https://www.govinfo.gov/content/pkg/USCOURTS-ilnd-1_15-cv-10889/pdf/USCOURTS-ilnd-1_15-cv-10889-1.pdf hereinafter *VTech*.
[1195] *Vtech*, 4.
[1196] *Vtech*, 4.

than 500 euros, the PLD could have applied. Given the vulnerability status of children, a CJEU judge would probably have applied an abstract level of the defectiveness standard in Article 6 PLD to the defect of these toys.

Even if the Judge did not accept any of the plaintiffs' arguments, there are several passages that can also be of interest for the discussion of the US product liability theories applied to the IoT domestic objects. Firstly, the judge did not accept the plaintiffs' reasons on the first count (breach of contract)[1197]. In fact, the plaintiffs argued that they had entered a contractual relationship with *VTech* by purchasing the toys. They then claimed that *VTech* had actually implicitly promised that these interactive devices would supply Internet services in a continuous way and with a high level of data security. Moreover, *Vtech* had claimed that children's data protection would be complete because of the use of "*effective and industry standards security measures*"[1198]. Nevertheless, the plaintiffs were not clear on which of three possible contracts these promises concerning the online service were based.

According to Judge Shah, there were three contracts: the first became effective on purchase of the toy; the second was the terms and conditions of the Learning Lodge and Kid Content, the interactive platform that allowed children to play with the toy and communicate with friends and parents, and the last one was *Vtech*'s privacy policy, which was incorporated by reference into the Online Service contract. Despite the existence of these three contracts, the plaintiffs did not label either these contracts as the ones that were breached or *Vtech*'s promises as being either implicit or explicit. The judge deemed that both the contract nature and promise were *de facto* implied by the plaintiffs. However, Judge Shah explained that where there was an implied contract of purchase, by the plaintiffs, there was also an explicit one: the online services contract[1199]. It was not possible for an implicit contract and an explicit one to coexist, hence the explicit one had to prevail.

Consequently, as the plaintiffs could not characterise the breach of contract as a breach of an online services contract, they also could not prove their following claims. For instance, as far as the continuity of access to online services was concerned, the interruption of services alleged by the plaintiffs could not be based on an implicit contract, but by expressly referring to the online services contract[1200]. The same reasoning applied to the lack of data security effectively provided[1201]. In suborder to the breach of contract claims, the plaintiffs tried to demonstrate that there had been a breach of an implied warrantee of merchantability, but they were unsuccessful due to the contract issue already discussed, which was considered as preliminary for deciding all the other claims[1202].

[1197] *Vtech* 6-9
[1198] III Analysis a) breach of contract.
[1199] *Vtech* 6-9
[1200] *Vtech* 6-9.
[1201] *Vtech* 6-9.
[1202] B. Breach of implied warranty of Merchantability (Counts III-IV), 10-14.

Before reaching this conclusion, Judge Shah's reasoning over the concept of interconnected goods, such as IoT toys, should be highlighted. Judge Shah made the following reasoning: while the contract in this case was about online services, those same services would have been useless without the physical support of the toy, hence the smart toy could be recognised primarily as a good[1203]. It is interesting that the reasoning of the American judge arrived at the same conclusion as some European legal institutions over connected goods, such as ELI[1204]. This stance seems to be a minority one in the US, as software is primarily considered a service[1205]. However, it was explained in 2.3 that some scholars, Professor Elvy in particular, advocate for a functional concept of product/good, which, in some cases, could also include its software parts[1206], as Judge Shah *de facto* did in this judgment.

Despite the unsatisfactory result of the parents' class action lawsuit, the FTC started a complaint against *Vtech* two years after this judgment[1207]. The complaint contains the "usual" allegations of the infringement of Section 5 of the FTC Act as *VTech* had misrepresented the security of its toys, or, as they are called in the complaint Electronic Learning Products (ELPs) and had failed to encrypt the communications among these ELPs[1208]. Moreover, given that children were involved[1209], the COPPA[1210] was applied and the FTC is also the government body entrusted with its application. This meant that in this case, the FTC could issue monetary fines. Hence, the FTC alleged the breach of the COPPA rule by *VTech* as the platforms Learning Lodge, Kid Connect[1211] and Planet *VTech* did not respect COPPA rules on data privacy concerning children. For instance, one of the claims is that the *VTech* Privacy Policy was not clear about data/personal information collection on minors[1212]. The other most relevant claim was that *VTech* did not provide the necessary data security for children personal information[1213] as the hacker[1214] could access so many minors' personal data.

Apart from the injunctive remedies that follow the main features of the previously commented ones in subsection 3.1.1.[1215] of this chapter, the order

[1203] *Vtech* 10.
[1204] See Chapter V, Article 2 PLD.
[1205] International Encyclopaedia of Cyber Law,"§4. INTERPRETING SOFTWARE CONTRACTS" 5813249 (C.C.H.), 2020 WL 5813249
[1206] Stacy Ann-Elvy (2021),316-318.
[1207] VTech Electronics Limited, Accessed 31 January 2023, https://www.ftc.gov/system/files/documents/cases/vtech_file_stamped_complaint_w_exs_1-8-18.pdf (hereinafter *VTech Complaint*); https://www.ftc.gov/system/files/documents/cases/vtech_file_stamped_stip_order_1-8-18.pdf (hereinafter *VTech Stipulated Order*.
[1208] Count II, *VTech complaint*.
[1209] §§17-19 *VTech complaint*.
[1210] §5 *VTech complaint*.
[1211] (These two were the same platforms of the judicial case *VTech*)
[1212] §23 *VTech complaint*.
[1213] §25 *VTech complaint.*
[1214] The same one cited by *Vtech* judicial case.
[1215] There are for example: an injunction to respect the COPPA rule when exercising data collection operations (I); an injunction regarding the misrepresentation of data security and privacy practices (IV), a requirement to establish and implement a comprehensive data security program requirement (V) and its assessment (VI), record keeping obligations (IX) and compliance monitoring (X). *VTech Stipulated order*

differs due to the fact that one of the bases of the claim is also the applicability of the COPPA Rule. It was because of the applicability of COPPA that the FTC could also ask for the payment of a civil penalty of $650,000[1216], plus additional monetary provisions as an application of bankruptcy law. In the end, *VTech* accepted the settlement, which coincided with the instructions contained in the order.

In the end, it appears that the courts require claimants to give evidence of a higher standard in order to demonstrate harm from an IoT toy, even when contractual law and not just data protection law is applied, as in this case. Even if neither standing issues nor *Clapper* were mentioned, in this case the court considered that a preliminary element (the identification of the right contract from which harm derived) was actually able to determine the outcome of the case. Even though this was not a procedural rule such as the one of Article III and the definition of injury in fact, the final effect was the same. On the contrary, The FTC focused on the application of the COPPA and interpreted the provisions infringed through the wide meaning of misrepresentation in Section 5 of the FTC Act. Therefore, the harm caused by the hacker could even have not taken place and the FTC would have been involved anyway.

3.2.2. Archer-Hayes v. Toytalk, INC.

Another interesting case involving interactive IoT toys is Ashley ARCHER-HAYES, v. TOYTALK, INC[1217]. This case also involved IoT devices for children. In particular, it concerned the partnership between the manufacturers of popular doll Barbie and the company Hello Talk, specialised in speech recognition and interactive programmes for kids. Through this doll, it was possible for the child (aged 6 and older) to speak and talk with Hello Barbie and have “real” conversations with the toy.

Hello Talk advertised that it would not share the recording logs with third parties unless parents shared the recordings on their social media. This product had also obtained the KidSafe+ label[1218] and it was meant to respect all the provisions concerning the Children Online Protection Act (COPPA). Unfortunately, according to the plaintiffs, that was not the case: when other children (besides the child-owner of the smart doll) played with and spoke to Barbie HelloTalk, the doll recorded the voice of the other minor. The problem was that the minor’s parents who did not own the doll may not have given their consent for the recording of their child’s speech.

The plaintiffs alleged several counts, the first of which was violation under unfair competition law, because both Mattel and Hello Talk produced a

[1216] II and III, *VTech Stipulated order.*
[1217] Archer-Hayes v. ToyTalk, Inc., No. BC603467, 2015 WL 8304161 (Cal. Super. Dec. 7, 2015), hereinafter *Archer-Hayes*.
[1218] §19 *Archer-Hayes*.

misleading advertising of the doll and should have known that the doll recorded other children's voices. Plaintiffs also claimed that, had they known that the doll should not be shared among children, they would not have purchased it[1219]. The second count, instead, is about the producer's negligence. According to the plaintiffs there are several duties of care that Toytalk and Mattel breached. For instance, Toytalk allegedly breached the duty "*to use reasonable means to implement a process by which they could prevent such collection or delete such recordings*"[1220], and also to rapidly notify affected individuals in order to receive their consent. The third count is based on unjust enrichment which basically states that by selling an unlawful product, which could constitute a danger to children, HelloTalk had made gains in an unfair and unlawful way[1221]. The last one, on the other hand, is a privacy tort. Specifically, it was invasion of privacy. Regarding this last count, the plaintiffs claimed that they "*had a reasonable expectation of privacy*" and believed, as the manufacturer had advertised, that audio recordings of children without parents' consent would not be collected stored, used and shared with third parties[1222]. However, it is not clear why this lawsuit was dropped. It is possible that the defendants reached a settlement with the plaintiffs.

3.2.3. A comparison between Archer-Hays and V-Tech and EU law

The *Archer-Hays* and *Vtech* judgments are similar as they were both class actions to recover damages or reverse unjust enrichment resulting from smart toys. Nevertheless, these judgments also differ in several other aspects. First of all, the COPPA played a different role in each of the judgments: in *Archer Hays*, the plaintiffs did not use it as the toy had obtained the label that certified its compliance with COPPA. If the parents in *Vtech* had used it as leverage, they might have obtained better results than relying solely on contract law, as instead they did by relying on the implied merchantability warranty and the data security arguments. However, the *Archer-Hays* plaintiffs could rely on the California Unfair Competition Law Act (which was also reminiscent of Section 5 of the FTC Act in its phrasing) and the unjust enrichment claims to obtain the same result. Moreover, in *Archer-Hays*, it is the first time that negligence and the breach of duty of care is actually used by plaintiffs to make their case when smart toys are involved. It can be inferred that this action also intended to demonstrate the inherent defectiveness of the product, hence its reliance on some of the theories discussed in 2.1. The same could be said for *VTech* and the claim about the merchantability warranty. As there are many theories about it as explained in 1.1, it is unlikely that a judge refers to products liability in general, as could be expected in the EU. Another difference between these two judgments is that in *Vtech,* a hacker actually accessed the data. Nevertheless, it was unclear whether it had misused the personal information acquired before being arrested, and this has relevance in all the judgments concerning data privacy harm, as shown in

[1219] §§ 29-38 *Archer-Hayes*.
[1220] §41 *Archer-Hayes*.
[1221] §§ 47-48 *Archer-Hayes*.
[1222] §55 *Archer-Hayes*.

Onity. However, by recalling the comment in *Onity*, sometimes courts do not recognise harm even when there is notice of an actual subsequent misuse of personal information. In *Archer-Hays*, instead, there was no news of a hacker. It was probably more prudent of the plaintiffs not to mention theories of intangible harm, they instead made the case on the invasion of privacy tort and a legitimate expectation about that aspect.

Regarding EU law, one can wonder how the CJEU might have judged these cases. Firstly, I would have expected parents to report the toys to the RAPEX system so they could possibly be recalled from market. Moreover, NPDAs or competition and consumer national authorities might also have started their own investigation on the issue. Otherwise, one could frame the legal issues as both product liability and data protection issues. Regarding the product liability evaluation, it is unlikely the PLD could be applied as there were no physical injuries, there was no damage to property and in any case, the economic damage is unlikely to meet the monetary threshold of Article 9(b) PLD. One could always use national product liability theories in combination (or not, depending on the MS) with the national implementation of Article 82 GDPR concerning the liability from data breach, but it might also be difficult to prove the damage from data breach, as MS judges' views on these issues might differ greatly from one country to another.

3.3. Medical devices and IoT with medical functions

This sub-section focuses on the cases regarding IoT with medical devices functions. There are two main reasons to also focus on healthcare IoT objects despite not being the main focus of the thesis. The first is that IoT with medical functions and IoT with consumer/domestic functions are receiving increasing investments[1223]. However, in the US, as already suggested in Chapter II, there is the start of a cross-over, a hybridisation between consumer and healthcare functions in IoT objects. As proof that this is a valuable market, consider the fact that Amazon has been investing not only in smart services to ship pharmaceutical products (read smart transport, or IoT-powered transport), but has also acquired Onemedical, a network of primary health clinics providing e-health services[1224]. This would mean that there will be the need for new smart objects such as phones, or other wearables that could monitor body functions (they already exist but they mainly have a health fitness purpose in the home) to carry out medical examinations while being connected to a doctor. This kind of private service will

[1223] IMC Newsdesk, "Digital health investments surge 79 per cent," *imc, IoT M2m council*, Accessed 31 January 2023, https://www.iotm2mcouncil.org/iot-library/news/connected-health-news/digital-health-investments-surge-79-per-cent/.

[1224] Sheila Zabeu, "Amazon buys One Medical, subscription health services company," NETWORKKING. The IT Monitoring Magazine, July 25, 2022, https://network-king.net/amazon-buys-one-medical-subscription-health-services-company/#:~:text=Amazon%20buys%20One%20Medical%2C%20subscription%20health%20services%20company,-Sheila%20Zabeu&text=After%20Oracle's%20largest%20acquisition%20completed,for%20another%20shot%20from%20Amazon .

be in competition with e-health services that hospitals would be able to provide. Even if in the EU there is a specific regime for medical devices, the Medical Devices Regulation (MDR), in the future the boundary between commercial and health IoT within the home might not be so strictly defined. Moreover, as I will explain in 3.3.2, II. the liability regime for IoT-medical devices and IoT domestic/commercial products may be largely the same. As a consequence of the insights that this could bring in the future, one can understand the importance of analysing the kind of claims IoT with medical functions that could be used at home are bringing to the US courts.

This sub-subsection is divided into two parts. The first one is more anecdotic and briefly tells the history of what could be considered to be one of the first IoT objects with medical functions as also a tragic history in terms of products liability (3.3.1). The second part instead focuses on a series of products liability cases involving the same manufacturer, St Jude Medical LLC, which designs implantable medical devices for pain management that can be directly controlled by the user through a remote. The fact that there are sensors and possibly a form of electromagnetic connection between the remote and the device makes it an IoT according to the definition of the Internet of Things Cybersecurity Improvement Act of 2020, as they most probably have a transducer (sensor or actuator), a network interface (the program on the patient's remote and the software programme for the doctor/technician to check remotely) and are able to work on their own (3.3.2).

3.3.1. The Therac-25 Case. An ante litteram IoT case

One of the first ever known medical IoT cases and scandals concerned a device that could be considered an IoT *ante-litteram* because it dates back to the '80s. It is known as the *Therac-25* case[1225].

Therac-25 was a machine used in radiotherapy to treat cancer and it was the first one to be controlled by a software programme. It was originally built in Canada, but the product was used also in the US by several health institutions. Due to an engineering and a software programme defect, some of the people who were treated with *Therac-25* started experiencing burns and at least three of them died[1226]. It is quite difficult to find judgments on the Internet about Therac-25, as the name of the victims may have been kept private and lawsuits could possibly have been settled by the producer (Atomic Energy Canada Limited). In any case, if we bear in mind that the first recognised IoT was a toaster connected to a portable computer[1227], then also the *Therac-25*, which was labelled primarily as a radiotherapy machine, hence a medical device, was also an IoT with medical functions.

[1225] It was cited in 2.3 of this Chapter by the scholar Karni Chagal-Feferkorn.
[1226] "Therac 25," Wikipedia, Accessed 31 January 2023, https://en.wikipedia.org/wiki/Therac-25.
[1227] See Chapter II.

3.3.2. The St Jude Medical LLC cases

Before delving into the cases, it is important to have a few facts in order to better follow the legal reasoning developed in each of them.

All the following cases involve the same producer of medical devices (medical IoTs), St. Jude Medical LLC. It produced several implantable medical devices with different names. The ones at issue in the four cases were spinal cord stimulators, focused on pain management, especially after back surgeries (e.g., hernia cases). From the cases at hand, it appears that the devices were structured in this way: there was an implantable part (made of octrodes and, possibly, of some kind of sensors) which was supposedly able to relieve the pain through electromagnetic waves. The patients had a sort of remote with a display which allowed them to regulate the intensity of the implanted part's activity and also be alerted in case of technical failures (e.g., low battery level or other technical problems). It also seemed that the doctor and technicians at St Jude Medical had a software programme with which they could check on the device and run the main settings of the device from there as well. Could they also be considered IoT? According to Gorman, yes, as they used an "*in-home monitoring system and use of radio frequency wireless technology*"[1228]. In any case, none of the following cases had data privacy and data security issues, but products liability claims.

Some of St Jude Medical products, specifically EON I Ipg and EON II Ipg, were recalled from the market due to of battery failures. There are four cases in total involving defective implants that were distributed from 2014 and that lead to legal actions from patients around 2019 and 2020, with judgments being rendered from 2019 to 2021. Moreover, all four cases were judged by the same person (Judge Burke) in the State of Delaware. I decided to split the subsection into two parts. The first one concerns how the theme of pre-emption for medical devices connects with product liability theories (3.3.2., I). In the second part, I try to outline the main differences between the American and the EU medical device regulation systems and I will try to understand what the further evolution of these systems is with the growing importance of IoT medical devices that could be used from home (3.2.2., II).

I. American pre-emption and the St. Jude Medical LLC cases: Freed III, Mellott, Guinn and Ross

The first two judgments are called *Freed v. St. Jude Medical LLC*[1229] and *Mellot v. St. Jude Medical LLC*[1230]. In reality, the *Freed* judgment is actually the last step of a longer series of suits involving the same plaintiffs (the Freeds) and

[1228] Leta Gorman, "The Era of the Internet of Things: Can Product Liability Laws Keep Up?," *Defense Counsel Journal* 84, 3(2017):7.
[1229] Freed v. St. Jude Med., Inc., Civil Action No. 17-1128-CJB, 2019 WL 5102643 (D. Del. Oct. 11, 2019), hereinafter *Freed III.*
[1230] Mellott v. St. Jude Med., LLC, Civil Action No. 19- 1779-CJB (D. Del. Nov. 16, 2020) (D.I. 45 at 7-8, 9-14), hereinafter *Mellott*.

the same defendant, St. Jude Medical LLC. However, I prefer to focus on *Mellot*, which was rendered a few months after *Freed III* in 2019, as it better explains how the issue of pre-emption connects with products liability theories when discussing medical devices.

Mr Mellot had sustained an injury in his lower back while working as a policeman in 2011 and thereafter experienced a huge amount of pain[1231]. In 2012, it was suggested he undertakes a trial period with the St Jude Medical LLC spinal cord simulator (Eon IPG) by his doctor[1232]. After a positive experience with the trial, Mr Mellot underwent surgery in the same year and the Eon model was implanted. He was reinstated to full duty at the beginning of 2014[1233]. However, in July 2014 he received a letter from St Jude which offered a replacement charger given that there might be problems of "*excessive warmth or heating at the implant site during the charging" of the Eon device*"[1234]. Until that point in time, Mr Mellott had not had any problem with the device[1235]. However, two years after receiving the letter he went back to the doctor stating that the device was overheating while charging and that sometimes the stimulation would suddenly increase automatically and then abruptly shut off and this required the device to be manually reset[1236]. After a meeting between the patient, the doctor and a St Jude technician, the doctor recommended that the old battery be explanted, and a new Eon IPG be implanted. During a second surgical procedure at the end of 2016, Mr Mellott had a new model of stimulator implanted, the Protégé. However, in 2017, things turned even worse for Mr Mellott: the second device turned on and off spontaneously without any advance notice and that made Mr Mellott feel intense pain in his back and left leg. Even though Mr Mellott informed St Jude of these problems, no solution was found.

Because of his deteriorated health condition and the pain experienced, Mr Mellott was not permitted to continue working as a police officer. This led to retirement due to disability. Hence, Mellott argued that St Jude was liable under strict liability, as its devices were manifestly defective[1237]; the second count was based on negligence, as St Jude manufactured devices with components that were defective and that the recall campaigns for other spinal cord stimulators that St Jude had made in the past should be considered as an indicative sign that its products could be defective[1238]; finally, Mellott alleged that the manufacturer was liable because of its failure to warn the plaintiff. This claim was divided into two parts: the first one concerned the failure to "sufficiently update or change its labelling" and the second one that St Jude failed to report adverse events to the FDA[1239] .

[1231] Mellott,4.
[1232] Mellott,4.
[1233] Mellott,4.
[1234] Mellott, 5.
[1235] Mellott, 5.
[1236] Mellott,5.
[1237] Mellott, 14.
[1238] Mellott, 15.
[1239] Mellott, 26.

The *Freed III* judgment is more succinct on the facts of the case, as there were previously two complaints[1240] that the judge asked to amend but I could not retrieve the text of these previous judgments. However, it could be inferred from the third judgment that Mrs Mellot had undergone a surgical procedure to implant a St Jude Medical spinal cord stimulator The Protégé sometime after 2014. It was not possible to retrieve the previous judgments *Freed I* and *Freed II,* but it is legitimate to infer from the text that the plaintiffs had experienced a problem with batteries. The claims made are almost identical to *Mellott*, as there is a negligent manufacturing claim[1241], and a failure to warn claim[1242].

One important aspect common to both these judgments is that the defendant, St Jude Medical LLC, had tried to make all the claims of the plaintiffs invalid by alleging that the plaintiffs had not sufficiently demonstrated that their claims were not pre-empted. This defence can be understood only by (briefly) explaining how the Medical Devices Amendments Act works and how it was interpreted by the US Supreme Court.

The Medical Devices Amendments Act (MDA) of 1976[1243] divides the medical devices into three classes of risk. According to the level of the risk (low, medium-high, high) there will be different procedures involving FDA checks. The three main ways through which the FDA regulation markets the medical devices are the following: Pre-market Notification (better known as 510(k) clearance), Pre-market Approval (PMA) and Humanitarian exemption[1244]. However, the medical devices at hand are included in Class III and are subjected to the most pervasive and encompassing form of FDA control: the PMA. On completion of each PMA, the FDA authorises the device for the market because the manufacturer's application successfully demonstrated their compliance with the Class III requirements as far as the manufacturing process, the design, the safety and the effectiveness of the device[1245] were concerned. The American system of medical device authorisation is known to be in general longer and more rigid than the European one for checking medical devices. Even though the EU system has been criticised for not making patients' health a priority over industry ambitions

[1240] The First Amended Complaint (FAC) and the Second Amended Complaint (SAC), *Freed* III,
[1241] *Freed,* III, 2.
[1242] *Freed,* III, 5.
[1243] "Medical Devices Amendments Act, May 28 1976, Public Law 94-295, 94th Congress,"*U.S. Food and Drug Administration*, Accessed 31 January 2023, https://www.govinfo.gov/content/pkg/STATUTE-90/pdf/STATUTE-90-Pg539.pdf .
[1244] The different procedures depend on the classification of the object in one of the three aforementioned classes. If the risk is low, then there is no formal testing. If there is a moderate risk and/or substantial equivalence to another product already approved, then there can be 510(k) clearance. If the producer of the medical device manages to prove that there is a substantial equivalence with an already marketed medical device or that was in use before the 28 May 1976 (which is the date of enforcement of the aforementioned Medical Devices Amendment Act) then it can avail itself of this method. If one starts this process, no clinical study is required. On the contrary, if the device presents a novel design and/or a high risk for the body, premarket approval is required which needs the support of clinical test trials through the process of pre-market approval. If this process is successful, the FDA authorises the marketing of the product in all the US. See Madelyn Lauer, Jordan P. Barker, Mitchell Solano and Jonathan Dubin, "FDA Device Regulation," *Missouri Medecine* 114,4(2017): 285.
[1245] Demetria D. Frank-Jackson, "THE MEDICAL DEVICE FEDERAL PREEMPTION TRILOGY: SALVAGING DUE PROCESS FOR INJURED PATIENTS," *Southern Illinois Law Review* 35(2019):455-456, hereinafter, Frank-Jackson.

and gains[1246], it has been remarked that the EU health systems are still considerably under national competence "*and that country payors are generally more aware of what they buy, whereas…., once new drugs or devices enter[in] the [American] system, is more difficult to block them, even though this does not mean that the FDA cannot recall defective medical devices*" [1247]. Moreover, we will see that the two systems might have been more similar than thought, if only legal remedies are considered (see 2.3.2. II below)

The doctrine of federal pre-emption is founded on the supremacy clause of the constitution of the United States and states that it will trump conflicting state law. The MDA section 360k sets a federal pre-emption clause in which it establishes that States are not allowed to introduce new or conflicting requirements involving Class III medical devices, as they will be pre-empted. St Jude Medical products belonged to Class III and that is why its main defence against the complaints was federal pre-emption. The problem with this system is when the medical device turns out to be defective even after the PMA. The state requirements mentioned in section 360 k of the MDA arguably also include remedies that might be more favourable to plaintiffs. If, then, as in the following cases, the medical devices are defective despite the PMA, the plaintiffs have virtually no remedies under their state law and medical device manufacturers are actually exempt from liability in practice. Originally, the rationale of the rule was to balance the higher compliance burdens of high-risk medical device manufacturers from a potentially wide array of state requirements. The US Supreme Court interpreted this exemption in narrow way through an evolution of three cases: *Medtronic v. Lohr[1248]*, *Buckman v. Plaintiffs' Legal Committee[1249]* and *Riegel v. Medtronic[1250]*.

As amply explained by judge Burke in *Mellot*, *Riegel* established the following principles: "[…] *In light of Section 360k(a), the Supreme Court of the United States has construed the MDA as protecting Class III device manufacturers from liability under state law tort claims if the manufacturer has complied with federal regulatory requirements*" [1251]. Therefore, in order to demonstrate whether a claim is expressly pre-empted, the court must evaluate two elements[1252]. Firstly, according to *Riegel,* the court must determine whether the FDA has established requirements applicable to the medical devices at issue[1253]. Secondly, it must determine whether the plaintiff's state law claims relate to safety and effectiveness and impose requirements that are "different from or in addition to" those imposed by federal law[1254]. The only exception contemplated in *Riegel* is when the state requirements "parallel" federal

[1246] Holly Jarman, Sarah Rozenblum and Tiffany J. Huang, "Neither protective nor harmonized: The crossborder regulation of medical devices in the EU," *Health Economics, Policy and Law* 16,1(2021):51-63.
[1247] Madelyn Lauer at al. supra.
[1248] Medtronic v. Lohr, 518 U.S. 470 (1996). Hereinafter *Lohr*.
[1249] Buckman v. Plaintiffs' Legal Comm., 531 U.S. 341(2001), hereinafter *Buckman*.
[1250] Riegel v. Medtronic, 552 U.S. 312 (2008). Hereinafter *Riegel*.
[1251] *Mellot*, 11.
[1252] *Mellot*,12.
[1253] *Mellot*,12.
[1254] *Mellot*,12.

requirements. However, even in this case, the plaintiff must plead facts which demonstrate action or inaction of the defendant's effort to take part in the PMA process or implement its result[1255].

In *Freed III*, the judge considered that the plaintiffs "negligent manufacturing" claim was justified. In order to avoid federal pre-emption, in the Second Amended Complaint (SAC) the plaintiffs had argued that the FDA good manufacturing practices (GMP)[1256] had not been respected by the defendant, hence the medical device was sold to them altered[1257]. The defendant in the oral arguments noticed that this claim was the same as in the First Amended Complaint (FAC) but the judge did not accept the two new reasons that the St Jude counsel added in the oral argument, which should instead have already been present in the FAC according to Article 12(g)(2) of the rule of procedure[1258]. The plaintiffs were also successful as far as their second claim: the failure to warn. In fact, in the SAC, the Judge had already considered the causal link between St. Jude's failure to report adverse events and Mrs Freed's injuries[1259]. In the last complaint, instead, the plaintiffs claimed that if St. Jude "*had properly informed or notified the FDA of the spinal cord stimulator devices' hazards risks and defects, Mrs Freed and/or her physicians would have learned about them and either chosen to implant a different neuro-stimulation system or taken steps to avoid the use of the spinal cord stimulator device in a specific manner or environment that created the risk of harm*"[1260]. The Judge considered this explanation satisfying and dismissed the defendant's rebuttal that the recalls and warnings had concerned other spinal cord stimulators manufactured by the defendant, but not the one which had been implanted in the defendant's body, hence they were not useful in proving causation[1261]. In fact, the Judge considered that by pointing out the recall of other products, the plaintiffs had demonstrated the failure to warn claim: in fact, on March 21, 2014, the FDA had approved a St Jude PMA supplement, the effect of which was to simply change the name of the "Eon Mini" device to the "Protégé" device, which was the model implanted in Mrs Freed's body. This made the devices mechanically identical. If this had been known, the physician might have suggested a different solution for Mrs Freed. Hence the causal link was proved[1262].

The *Mellott* judgment outcome is instead more varied. Some claims from the plaintiffs were not admitted by the judge and others were accepted. For instance, the judge rejected the plaintiff's strict liability claim as it did not specify which federal violations had been violated, hence the issue was pre-empted[1263].

[1255] *Mellot*,13.
[1256] U.S.C. §351.
[1257] *Freed* III, 3
[1258] *Freed* III, 3-5.
[1259] *Freed* III, 5.
[1260] *Freed* III,6.
[1261] *Freed* III,7.
[1262] *Freed,* III,9.
[1263] *Mellott*, 14-15.

With regard to *Mellott*'s negligence claim, the reply was more structured. One of the issues to solve, as in the *Freed III* judgment, was how to judge Mellott's claims about whether the recall of the Eon stimulators exempted the plaintiff from pre-emption[1264]. The Judge considered that the plaintiff used the recalls of the previous device type Eon "*as one part of a larger evidentiary whole that led to the possible conclusion that St. Jude's devices were negligently manufactured*"[1265]. Moreover, by relying also on *Freed III*[1266], the judge repeated that the FDA approved a labelling identification that simply changed the name of the Eon IPG to Protegé. Hence the products were mechanically the same. However, the judge agreed on St Jude's objection that the Eon recalls were connected with alleged defects that were different from what Mr Mellott had experienced with the second implanted device, the Protégé[1267]. In brief, the plaintiff failed to show how "'*the IPG […] losing ability to communicate with or recharge the IPG' is the same thing as, or somehow linked to, the IPG turning on and off spontaneously*."[1268] Hence this part of the negligence claim was insufficiently motivated by the plaintiff. Instead, the Judge considered that, regarding the negligence claim concerning the Eon Device (the first one that was implanted in Mr Mellott's body), the plaintiff sufficiently motivated his claim[1269]. This part of the judgment is particularly interesting as Judge Burke analysed the US Supreme Court's and the national court's views on how to interpret FDA good manufacturing practices (GMP) which also refer to Class III devices. St Jude was convinced that these are just guidelines that are too general and open ended to be considered effective federal requirements in order to demonstrate whether pre-emption can subsist or not[1270]. However, the judge and other courts disagreed on this point and considered the GMP as effective federal requirements, and that "[…] *a holding that GMPs are too vague to support a non-preempted claim would leave injured patients without any remedy for what could amount to a harmful violation of federal law*."[1271]

With regard to the duty to warn, the judge found that the defendant could not substantially prove the claim based on the duty to supplement labelling theory because the plaintiff used the *Mensig* judgment, in which the manufacturer had a lighter labelling duty at federal level than at the national one, improperly, hence the plaintiffs' claims in that case were pre-empted[1272]. However, in the case at hand, St Jude was not a drug producer but a medical devices manufacturer, hence was permitted, without approval from the FDA, to change the label of its devices. Nevertheless, the judge did not deem that the plaintiffs had proved enough information that the defendants knew that both the devices had battery problems but failed to alert the FDA. This claim was made under Section 388, with reference to both devices[1273]. In the end, in this judgment both the plaintiff

[1264] *Mellott*, 16.
[1265] *Mellott*,16.
[1266] *Mellott*,18.
[1267] *Mellott*,18.
[1268] *Mellott*,19.
[1269] *Mellott*, 21.
[1270] *Mellott*, 22.
[1271] *Mellott*, 22.
[1272] Mellott 26-27 citing PILVA, Inc. V. Mensing, 564 US 604, 618-19 2011, hereinafter *Mensing.*
[1273] *Mellott*, 28.

and the complainant obtained the exact same amount of counts approved and denied.

The *Guinn* cases and the *Ross* case[1274] are in factual terms very similar to *Mellott* and *Freed III*. The plaintiffs had back injuries and had tried to relieve their pain with the implantation St Jude Medical LLC spinal cord stimulators (they had a different name, e.g. in *Guinn* it was named the Proclaim stimulator). However, they experienced the same kinds of failures as in *Mellott,* such as burning sensations when the device was charging and the autonomous turning on and off of the device. *Guinn* had the device substituted but to no avail, while Ross had it explanted and asked for redress. Both plaintiffs suffered economic prejudice (Guinn was laid off from work) due to of the consequences of their worsened health state.

The *Guinn* case in particular served as precedent of *Ross*. In her first complaint there were three claims: I) the first was a strict liability claim, II) the second was failure to warn according to the Washington's Product Liability Act (WPLA) as Ms Guinn was a resident of the state of Washington, and, finally III) negligence. Also in this case, St Jude pleaded that there was federal pre-emption. However, the first Guinn case was not successful for the plaintiff. The Judge in fact stated that "[w]*hile the plaintiff is correct in stating that the lithium battery in her defective stimulator and the ones that were recalled are actually the same,* [however,] *she did not provide the necessary information that would allow the Court to believe the upon information and believe assertion*"[1275]. In substance, the plaintiff's case was considered not well pleaded, hence the motion by the defendant was granted. After this unsuccessful pleading, Guinn however took the suggestion of the Judge and filed a second complaint, alleging facts of the kind suggested by the judge in the first judgment to prove her claims. Specifically, the second case was based on the failure to label the defective product correctly. For this reason, the pre-emption claims of the defendant had to be rejected. In this new Guinn case (Guinn II), the plaintiff was successful[1276].

The *Ross* twin case also had the defectiveness of the same kind of spinal cord stimulator: the Proclaim, as its subject. Basically, *Ross* took advantage of the ruling of *Guinn II* in order to structure its argument in the same way, namely using strict liability and negligence manufacturing as counts against the defectiveness of the device.

All four of these cases are important because they may still concern bodily injuries from implanted IoT medical devices, but IoT with healthcare functions will be used with increasing frequency at home in the framework of private or public hospital rehabilitation therapies, in order not to overcrowd hospitals, as instead happened at the beginning of the COVID-19 pandemic. One must then expect

[1274] Guinn v St Jude Medical LLC 20-71-CJB, D.I. 50 (*Guinn I*), Guinn v.St Jude Medical LLC, LLC 20-71-CJB, D.I. 77 (*Guinn II*) Colleen Ross v St Jude Medical LLC, N. 20-971-CJB (Ross).
[1275] *Guinn*, 15.
[1276] Guinn v. St. Jude Medical, LLC, N.20-71-CJB, 2021 (Guinn II)

that claims concerning data security and data privacy might add to products liability theories, whenever the IoT object will involve monitoring functions. Will eventual data privacy claims be subjected to the 360 k pre-emption clause? If there are different injuries (physical and harm from data breach) product liability claims might be kept separate from the privacy ones. In that case, the gravest injury might still need to overcome the *Riegel* doctrine on pre-emption; the data privacy claims will instead need to prove the immediateness and the in-factness of the harm according to *Clapper* and *Spokeo*.

II. Comparison with EU law: deciding which liability for IoT with medical and consumer functions

In 3.3.2. I, it was explained that the American medical device authorisation system could be considered more rigorous than the one adopted in the EU[1277]. After discussing the previous cases, it is clear that the US system also has its own shortcomings. In particular, the pre-emption clause of Section 360 K MDA could prove to be a two-edged sword. The manufacturers of Class III devices (which are the ones that could greatly impact patients' health) are *de facto* exempted from liability and the Supreme Court's interpretation on medical pre-emption in *Riegel* risks leaving citizens without effective remedies, as Judge Burke pointed out in *Mellot.*

This denial of remedies was the same result that occurred in the EU when the MDD was still applicable, in the context of the defective breast prostheses (PIP saga) scandal. The system was based (and still is to a certain extent) on the division of medical devices into several classes of risk, as in the US. Then for each class of risk, there is one or more procedures that the medical device manufacturer can choose from, all of which involve a NB. The NB are State-appointed certifying and auditing bodies which also receive competence from the EU Commission to evaluate medical device compliance with the MDD (now MDR). The appointment as an NB only takes place if the certifying/auditing body (which is often a private company) provides all the necessary information, meaning that it respects certain criteria, including independence and autonomy from the manufacturers. In Chapters II, III and V, the *Schmitt* judgment pointed out that in the event a fraudulent producer went bankrupt, the plaintiffs could not rely on the PLD. However, plaintiffs hoped for many years that national courts would interpret the MDD as a legal basis that recognised an implicit form of liability for the NB, in case it had been negligent in its assessment. The *Schmitt* judgment established that the Directive contained no such *proviso*, but that MS could apply a national role with the same effect, provided that the principles of equivalence and effectiveness with the EU law were respected.

To avoid this situation happening again, the new MDR has established several post-market surveillance duties[1278] and also several more requirements

[1277] Holly Jarman, Sarah Rozenblum and Tiffany J. Huang, "Neither protective nor harmonized: The cross-border regulation of medical devices in the EU," *Health Economics, Policy and Law* 16,1(2021):51-63
[1278] 83 MDR.

for NB. For instance, even if not liable for negligence, NB are responsible for the actions of their contractors and will be supervised by ad hoc national authorities[1279]. Also, manufacturers now have more duties. Among these, Article 10(16) MDR is particularly interesting as it states that producers must, "[…] *in a manner that is proportionate to the risk class, type of device and the size of the enterprise, have measures in place to provide sufficient financial coverage in respect of their potential liability under Directive 85/374/EEC, without prejudice to more protective measures under national law*". Even if this is an improvement compared to the lack of a similar provision in the MDD, this obligation does not specify which type of measures medical device producers should take to have enough resources to meet liability for defective devices. The most obvious measure would be civil liability insurance. However, since all of these measures will be governed by the applicable national rules on these issues, the possibility of insufficient coverage is not completely ruled out. Let us remember that *Allianz IARD* (the insurer) was not involved in the *Schmitt* case because the contract of insurance for PIP (governed by French law) was found to be void and null due PIP's fraudulent conduct, according to French law[1280]. It will be the Member States' responsibility to make rules that fairly balance the interests of insurances companies (which are not happy to bail out fraudsters or negligent producers at EU level, comprehensibly) and the expectations of consumers and patients about the protection of their health.

Why is discussing this so important? The MDR never mentions the IoT but does mention standards (harmonised or not). However, the fact that software could be considered a standalone medical device (Article 3.3, Chapter II, Annex VIII MDR) lets interpreters think that it will be applied to IoT with medical functions. Moreover, the connection of the PLD with Article 10(16) MDR is worth more careful reading. Despite the fact that the division between high- and low-risk technology is a constant in EU digital policy, from the proposed AI act to the Report on the Liability of AI and new technology of the Expert Group[1281], the PLD will become the generalised liability system in Europe, not only for consumer IoT objects , such as domestic IoTs, but also for healthcare IoT objects (which are generally considered high risk compared to consumer IoT) and also mixed IoT, with both healthcare and consumer functions, such as the smart watches that we wear. However, for healthcare IoT objects, Article 10(16) PLD establishes a special rule: the PLD must be applied "*without prejudice to more protective measures under national law*". This means that more protective national laws could apply thanks to the *Schmitt* judgment.

In the US, instead, even if the MDA has also been updated for new technologies by the 2016 *21st Century Cures Act*[1282] it appears that the *Riegel* doctrine will not allow many complainants to have access to effective remedies

[1279] Articles 35-37 MDR.
[1280] See Table I Chapter V for the story and main points of these judgments.
[1281] See Chapter III.
[1282] FDA, "A History of Medical Device Regulation & Oversight in the United States," FDA (Official Website), Accessed 31 January 2023, https://www.fda.gov/medical-devices/overview-device-regulation/history-medical-device-regulation-oversight-united-states .

whenever the medical device (and maybe medical IoT) proves to be defective. Moreover, another difference is that while the PLD is now the general EU liability instrument also for medical devices, in connection with national theories, in the US there will be no general liability framework for IoT objects. The products liability theories will continue to exist alongside new IoT objects provided that the pre-emption barrier is overcome.

3.4. Connected cars

There is a reason for distinguishing connected from autonomous cars. The cases that I am about to discuss concern recently marketed cars (at the beginning of the 2010s) by Toyota, Ford and General Motors. Connected means that they are not fully automated and autonomous. In fact, the majority of the cars I will discuss still require the driver to perform or to actively supervise the car, while, at the same time, its sensors and software assist cruising or perform other actions such as parking or acceleration. Hence, according to US National Highway Traffic Safety Administration (NHTSA) classification, these kinds of cars could be level 1 and level 2: that would mean that they are driver-assisted, or they allow partial automation of the car[1283]. Completely autonomous or driverless cars have been tested by several car manufacturers but none of them has been marketed yet as they are still too dangerous to drive [1284]. In the EU, fully automated cars will probably be part of a special regime[1285]. Despite this, even in the EU fully autonomous cars are not on the market yet because, at the moment, the risks still outweigh the benefits of this newly applied technology. However, this does not mean that the EU and European producers are not working to make fully autonomous cars a reality[1286].

The following cases are still relevant for the discussion as, even if not fully automated, the models concerned are equipped with sensors, actuators and displays that interact with the driver and the car manufacturer. Briefly, even if not fully automated and driver-less, the majority of new models of cars on the market

[1283] Calabresi and Al Mureden reported and explained to the NHTSA their division of the various kinds of driverless cars by considering their level autonomy. Level 0 is the traditional car while Level 1 is called "*driver assistance"* which also has tools such as cruise control, driver control and lane correction technology. Level 2 is called "*partial automation"* and concerns cars that control most of functions such as acceleration, but still have the option for the driver to intervene. Level 3 instead could be called "*conditional automation*" which could control every aspect of the drive limited to mapped environments but still the car would need a human pilot to monitor cruising and to intervene when necessary. Level 4 would be called "*high automation"* in which the presence of the pilot is already superfluous, but the pilot can take control of the car because it is not possible to drive autonomously or because they feel like driving. Lastly, level 5 is the one of "*full automation"* in which the car would not even require a driver within it. Guido Calabresi and Enrico Al Mureden, *Driverless cars* (Bologna: Il Mulino, 2021), 97-98.

[1284] Clifford Law Offices, "The Dangers of Driverless Cars," *National Law Review* 12,116 (2021), 5 May 2021, Accessed 31 January 2023, https://www.natlawreview.com/article/dangers-driverless-cars .

[1285] As indirect proof of that, the proposed AI act makes explicit in the explanatory memorandum that "[a]s regards high risk AI systems related to products covered by relevant Old approach legislation (e.g., aviation, cars) will not directly apply", AI Act, explanatory memorandum,4.

[1286] For a detailed reconstruction of the EU policy documents on autonomous cars and driving see Calabresi and Al Mureden. Guido Calabresi and Enrico Al Mureden, *Driverless cars* (Bologna: Il Mulino, 2021), 114-119.

can be considered as IoT objects. That is why I prefer to use the term connected car, instead of autonomous car. I will not focus on the dynamic of the car in the public space and on the surveillance aspects. Instead, I will try to analyse the connected car as a product, which is affected by both product liability rules and issues concerning data (whether personal or not).

The two cases are respectively the circuit court[1287] and the federal appeals court[1288] judgments involving the same plaintiffs (including the one who probably started the proceedings, Ms Cahen). The type of action that is used by the plaintiff is a putative class action. This kind of action consists of one or more plaintiffs starting an action on behalf of a group of people that is in a similar situation and have the same claim as the plaintiffs. However, it is indispensable that the putative class action is certified as such by the court and, in that case, that the initial lawsuit becomes a class action[1289].

With regard to the main claim, the plaintiffs argued that the car manufacturers had equipped their vehicles with computer technology that could be hacked by third parties[1290]. It is interesting to find a concise technological explanation of the problem shortly after. Each car was equipped with several electronic control units (ECUs) and the safety of those vehicles relied on these ECUs for communication with the manufacturer. This communication had a low latency time[1291]. The ECUs in fact are able to communicate inputs through a Controller Area Network (CAN bus), via digital messages called CAN Packets[1292]. The malfunctioning of this system had been known since 2011. This first main claim is followed by other several claims for the different putative class actions, originating in three different states (California, Oregon and Washington)[1293].

The other main claim was the infringement of the plaintiffs' privacy. The plaintiffs argued that defendants "*improperly collect and transmit information about vehicle performance and the geographical location of the cars they sell in violation of the plaintiffs' right to privacy*."[1294]

However, it must be said that for each of the inter- state class actions, there were more than the two formal claims that have just been described. It is worth analysing them more as they constitute relevant data on what subject IoT car product liability claims could have before the CJEU. The California Action contains very different claims, ranging from competition to constitutional law, and

[1287] Cahen v. Toyota Motor Corp., 147 F. Supp. 3d955 (N.D. Cal. 2015), Accessed 31 January 2023, https://casetext.com/case/cahen-v-toyota-motor-corp-3, hereinafter *Cahen I.*
[1288] Cahen et al v. Toyota Motor Corporation, Toyota Motor Sales, U.S.A., INC., and General Motors LLC, Case 16-15496,Accessed 31 January 2022, https://casetext.com/case/cahen-v-toyota-motor-corp-2, hereinafter Cahen II.
[1289] Putative Class Action, *IRMI*, Accessed 31 January 2023 https://www.irmi.com/term/insurance-definitions/putative-class-action.
[1290] United States District Court, N.D. California, Nov 25 2015, 147 F. Supp. 3d 955 (N.D. Cal. 2015).
[1291] As explained in Chapter II, latency is the property of an object to react as fast as the input is given. If an IoT product ha slow latency it means that there is the shortest amount of time between the moment the input is sent to the object and the object reaction.
[1292] *Cahen I* paras. 28-30.
[1293] *Cahen I* paras. 62-128.
[1294] *Cahen I* paras. 49-50.

from breach of state contract law to privacy torts. I will concentrate more on the Californian claims as the others are fewer in number. Moreover, the remaining interstate actions have very similar claims to the California ones, which is also the place of jurisdiction of this case[1295].

If we focus on the California claims[1296], it is interesting that claim 1) uses competition law as a means to protect the plaintiffs' interests (who are also consumers in this case) as in *Archer-Hays*. In particular, the competition claim states that the car advertisement was not truthful and that it led the defendant to have an unfair competitive advantage over other car manufacturers. Also noteworthy is claim 4), which is violation of the implied merchantability warranty that is part of California's transposition of the UCC. Yet again, competition is used to protect consumers (this time the FTC is not involved) and the implied merchantability warranty highlights the connection of this IoT object case to the mix of product liability theories discussed in 1.1. indirectly.

Lastly, it is important to remark on some similarities with previously cited judgments such as *VTech*, *Archer Hays* and *Onity* (which will be cited in the legal reasoning of Judge Orrick in *Cahen*), as far as the complaint structure is concerned. An element of similarity with *Vtech* and *Archer Hays* is the citing of national laws that protect consumers and also special fraud statutory regimes. The unfair competition/consumer protection element, intended as misrepresentation of the product and unfair practice (both at a national and at federal level), is present in all the previous FTC cases, but also in *Vtech* and *Archer Hays*. Furthermore, the tort of invasion of privacy is also present in the complaint in *Archer Hays*. The resolution of this case, however, is much more similar to *Onity* than the toys-related judgments.

Part A of Judge Orrick's reasoning is significantly labelled "*Whether Injury In Fact Exists Based On The Risk Of Future Hacking"*[1297]. That is because the issue of standing according to the federal laws of procedure was raised by the defendants and Judge Orrick argued that, on the basis of *Clapper* and *Onity* and another case *Birdsong v. Apple Inc*[1298]*,* the plaintiffs did not manage to prove the

[1295] In fact the Oregon class claims are the following (1) violation of Oregon's Unlawful Trade Practices Act, Or. Rev. Stat. § 646.605, et seq . ; (2) breach of Oregon's Implied Warranty of Merchantability, Or. Rev. Stat. § 72.3140 ; and (3) fraudulent concealment in Oregon common law. As far as Washington class action we can count: (1) violation of Washington's Consumer Protection Act, Rev. Code Wash. Ann. § 19.86.010, et seq . ; (2) breach of Washington's Implied Warranty of Merchantability, Rev. Code Wash. § 62A.2–614 ; (3) breach of contract in Washington common law; and (4) fraudulent concealment in Washington common law. *Cahen I* paras 62-138.

[1296] The complete list of claims for the California action is the following 1) violation of the California's Unfair competition law
2) violation of California's consumer legal remedies act
3) violation of California's False advertising law
4) breach of California's Implied Warranty Merchantability
5) breach of contract at California common law
6) fraud by concealment in California common law
7) violation of California's Song-Beverly Consumer Warranty act and 8) invasion of privacy under California Constitution. *Cahen I* paras 62-138.

[1297] Part A *Cahen I*, para 966.

[1298] Birdsong v. Apple Inc., 590 F.3d 955 (9th Cir. 2009), hereinafter *Birdsong v. Apple*. Cited by Judge Orrick*, Cahen I* at paras 966-969.

injury. Concerning *Clapper*, which is the federal precedent on standing, the federal requirement in order to prove standing is to prove that the damage (injury) is impending[1299]. This was not proved by the plaintiffs in the judge's view[1300]. Also, in *Birdsong,* the plaintiffs had tried to demonstrate the impendency of harm (the high probability of turning deaf as a consequence of the continuous use of an iPod) and were unsuccessful[1301]. Specifically, neither in *Birdsong* nor in *Cahen* did the plaintiffs manage to demonstrate that the injury was imminent/impending[1302]. Furthermore, the plaintiffs in *Cahen* did not prove how this impending injury was going to affect them, concretely and particularised "*as to themselves*"[1303]. Judge Orrick considered the suggestion of the plaintiffs' counsel concerning the judgment to take as a reference to solve the issue as misplaced[1304]. The counsel would have preferred for the judge to rely on the *In re MyFord Touch Consumer*[1305] litigation. Contrary to the present case, the judge states that the Ford models in *MyFordTouch* had a defect which concretely impacted the cars' functioning (which was also based on two major claims: fraud and breach of warranty). It was not like in the case at hand, where no actual harm had materialised[1306]. Moreover, the judge in *Cahen* also relied on the *Riva v. Pepsico, Inc* judgment[1307] and concluded that a speculative risk could not be considered as the cause of an injury, despite the injury being inferred whenever there is a "*a credible threat of harm*"[1308]. With *Clapper*, the credibility of the harm became connected to the certainty that a fact was impending in order not to consider the injury as too abstract and speculative[1309].

The second part (B) of the judgment concerns "*whether the damage exists based on the alleged economic loss flowing from the risk of future hacking*"[1310]. In the second subparagraph on the part dedicated to standing, the Judge, by relying on previous cases, showed that the claims of economic loss consequent to a very probable future hacking could not be accepted because the plaintiffs did not prove how a possible future injury could cause economic loss and also failed to quantify such loss in a satisfying manner[1311].

Once again, the claim was found not to have any standing: the plaintiffs used three judgments as bases for their claims: *Hinojos v. Kohl's Corp*[1312] and two other complaints involving Toyota: *In Re Toyota Motor Corp. Unintended*

[1299] *Cahen I* at paras 966-969.
[1300] *Cahen I* at paras 966-969.
[1301] *Cahen I* at paras 966-969.
[1302] *Cahen I* at paras 966-969.
[1303] *Cahen I* at paras 966-969.
[1304] *Cahen I* at paras 966-969.
[1305] *In re MyFord Touch Consumer,* 46 F.supp 3rd 945 (2014), hereinafter *MyFordTouch.* Cited by Judge Orrick*, Cahen I* at paras 966-969.
[1306] *Cahen I* at paras 966-969.
[1307] Riva v. Pepsico, 82 F. Supp. 3d 1045, 1052 (N.D. Cal 2015). Cited by Judge Orrick*, Cahen I* at paras 966-969.

[1308] *Cahen I* at paras 966-969.
[1309] *Cahen I* at paras 966-969.
[1310] Part B *Cahen I*, paras. 969-971.
[1311] *Cahen I*, paras. 969-971.
[1312] Hinojos v. Kohl's Corp, 718 F.3d 1098 (9th Cir.2013), hereinafter *Hinojos*. Cited by Judge Orrick*, Cahen I* at paras. 969-971

Acceleration Marketing Sales Practices and Products liability Litigation (Toyota I) [1313].Nevertheless, in *Hinojos* the items purchased were falsely advertised on sale: specifically, the seller had pretended to mark down the original higher price. In that case the economic injury was not speculative[1314]. On the contrary, in *Cahen*, the plaintiffs did not demonstrate that there was a misrepresentation of value, but alleged their cars were riskier, hence less valuable[1315]. Also, in *Toyota I*, it was reported that the acceleration defect in that model of car had been found several times[1316]. On this basis, that court could infer a market effect which was actual or imminent[1317]. Moreover, in the *Toyota I* case, the plaintiffs had relied on the Kelly Blue Book and other value guides to show that the value of the car had decreased because of the multiple recalls[1318]. Instead, in *Cahen*, the plaintiffs had made no specific allegations on what they would actually lose in the event that a third party hacked the car[1319]. In brief, the plaintiffs in *Cahen* failed to demonstrate the *"[…] 'something more' beyond the speculative risk of future harm that underlies the allegation of economic damage"[1320].*

The last part of the judgment addressed the concerns about the claim of "invasion of privacy"[1321]. This privacy tort was chosen because, according to the plaintiffs, the data collected by the model of car was not fair[1322]. Even if the owners of the cars knew and agreed to the defendant's privacy policy, they also concurred that it was not possible to opt out[1323]. Even for this angle of the issue, the rules concerning standing proved to be a filter against "future injury"[1324]. Judge Orrick also cites other cases and gives an outline of what an invasion of privacy should look like[1325]. For instance, it is necessary to identify a "*concrete form of harm deriving from the alleged collection and tracking of personal information*"[1326] and in any case, the plaintiffs in *Cahen* did not identify such harm, so they could not only rely on the tracking of their personal information to create an injury-of-fact based on *In re I-phone Application Litigation[1327]*. However, if there had actually been a theft followed by a data-breach caused by hackers, there could have been a "certainly impending" "credible threat" of future harm as established *In re Sony Gaming Networks & Customer Data Security Breach Litigation*[1328]. Moreover, the customers failed to identify a protected privacy

[1313] In Re Toyota Motr Corp. Unintended Acceleration Marketing Sales Practices and Products liability Litigation, 754 F. Supp. 2nd 1145 (C.D. Cal. 2010), hereinafter *Toyota I*. Cited by Judge Orrick*, Cahen I* at paras. 969-971.
[1314] *Cahen I*, paras. 969-971.
[1315] *Cahen I*, paras. 969-971.
[1316] *Cahen I*, paras. 969-971.
[1317]*Cahen I*, paras. 969-971.
[1318] *Cahen I*, paras. 969-971.
[1319] *Cahen I*, paras. 969-971.
[1320] *Cahen I*, paras. 969-971.
[1321] Part C *Cahen I*, paras. 971-974.
[1322] *Cahen I*, paras. 971-974.
[1323] *Cahen I*, paras. 971-974.
[1324] *Cahen I*, paras. 971-974.
[1325] *Cahen I*, paras. 971-974.
[1326] *Cahen I*, paras. 971-974.
[1327] In re I-phone Application Litigation No 11-MD-02250-LHK 2011 WL 4403963 *5 (N.D. Cal. Sept. 20 2011). Cited by Judge Orrick *Cahen I*, paras. 971-974.
[1328] In Sony Gaming Networks & Customer Data Security Breach Litigation, 996 F. Supp. 2nd 942 (S.D. Cal 2014), hereinafter *In Re Sony Gaming.*). Cited by Judge Orrick *Cahen I*, paras. 971-974.

interest among the two cited by the case *Hill v. Natl Collegiate Athletic Ass'n*[1329], which were notoriously divided into two classes: informational privacy ones and autonomy privacy interests[1330]. The former ones concern the interest in forbidding the sharing and misuse of sensitive and confidential information[1331]. The latter on the other hand concern personal decisions or activities without being afraid of being observed or of experiencing an intrusion or interference[1332].

This judgment is instructive as, a few years after *Onity*, the same line of reasoning concerning standing continued to be applied not only regarding the economic damage that could ensue by the state of potential "hackability" of cars, but also the alleged privacy invasion claim. It could all be summed up to the same principle, which is that one has to prove that a harmful fact has actually happened or is about to happen and that it needs to be proved. Ms *Cahen* decided to appeal the judgment. Not surprisingly, the Court of Appeals rejected the *Cahen* main claims by judging that Orrick's legal analysis was correct[1333]. It is interesting as even in the appeals phase, the issue of standing was important and a more recent US Supreme Court judgment such as *Spokeo*[1334] was used jointly with *Clapper* to establish that in this case, the plaintiff did not have any standing, also because she had failed to prove a causality link between a harm that was remote and the damage[1335].

3.4.1. Comparison with EU law

One might wonder why it is necessary to discuss about connected cars if they are not home objects. I did so because the cases analysed were actually consistent with my understanding of the IoT liability study in the US: as recalled in subsection 2.3, driverless cars were the perfect case study for US legal scholars to test their liability theories on AI-Robots-IoT[1336]. It would have been strange to exclude these recent cases from my analysis, especially because the cars discussed were not fully autonomous but let the user interact with them, as text-book IoT objects.

Moreover, my thesis is about domestic IoT in the EU and smart cars have a rather ambiguous status between the home as a private place and the city as a public place, but it is still a product that could be defective even if it will most

[1329] Hill v. Natl Collegiate Athletic Ass'n, 7 Cal 4th 1 (Cal.1994), 26 Cal. Rprt. 2d 834 865 P 2d 633.
[1330] *Cahen I*, paras. 971-974.
[1331] *Cahen I*, paras. 971-974.
[1332] *Cahen I*, paras. 971-974.
[1333] *Cahen II*, paras 1-5.
[1334] See *Onity* judgment in this chapter subsection 3.1.2.
[1335] *Cahen II*, paras 1-5.
[1336] Among many scholarly contributions I will cite here the work of Determann and Perens who used the autonomous car use-case to investigate the convenience to have an open car, meaning a car that "*supports an aftermarket in which third–party manufacturers produce accessories for the vehicle, including ones not envisioned by the original manufacturer*". They carry their research from several angles: from products liability to data privacy and from competition to intellectual property law. Lothar Determann and Bruce Perens, "Open Cars," *Berkley Technology Law Journal* 32,2(2017): 915-988.

likely be part of a separate and specific legal regime at the same time. In percentage, quite a relevant number of EU scholars devoted their research on tort law and strict liability of AI and IoT to autonomous cars, in the same way as their American colleagues [1337]. Furthermore, at first, tort experts devoted more attention to smart cars than to home smart appliances. Some of them have tried to suggest the possibility of creating compensation funds as alternatives to liability rules, making the example of connected cars and insurance companies are already dealing with connected cars[1338].

Moreover, the issue of car-generated data is actually also being discussed by representatives of European insurance groups and also with the EU institutions: they foresee changes in the E-privacy directive and a review of the EU motor insurance directive[1339]. It is arguable that there may be a more specific regime of data sharing inspired by the Articles 4 and 5 of the Data Act that could be applied to the connected cars[1340].

These cases are also interesting as they already show that data protection and economic-data exploitation claims will emerge together from this kind of litigation relating to "connected IoT cars". These cases also hinted that the software used by the car to perform its function is actually a product which works within the main one. This might push the idea that incorporated software is actually the same as a product. There are different kinds of personal data that could be accessed by hacking the car. There could be user IDs, email addresses, and insurance policy numbers. These groups of data will still be protected by the GDPR. Regarding liability, Article 82 GDPR ensures the compensation of both material and non-material damage entirely. I will redirect to Chapter V, and in particular the discussion on the future Article 9 PLD for a more complete discussion on the extent of the compensation of Article 82 GDPR[1341].

Finally, these judgments are also important because they shed a light on the so-called pure economic damage: the plaintiffs alleged that they had suffered economic damage as the car had the concrete risk of not performing as promised. This is important to bear in mind as it is a possibility that pure economic loss claims might also be filed in product liability complaints concerning IoT. Nevertheless, it must be remembered that not even EU judges would compensate pure economic loss for an intangible harm that has not yet happened.

[1337] Such as Professors Gerhard Wagner, Miquel Martín- Casals, Herbert-Zech, Giovanni Comandé Gerald Spindler, Ernst Karner, Bernard A. Koch, Cristina Amato, Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer. See their contributions In Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds.),*Liability for Artificial Intelligence and the Internet of Things Münster Colloquia on EU Law and the Digital Economy IV* (Baden-Baden: Nomos, 2020).

[1338] Georg Borges, "New Liability Concepts: the Potential of Insurance and Compensation Funds," In *Liability for Artificial Intelligence and the Internet of Things Münster Colloquia on EU Law and the Digital Economy IV* (Baden-Baden: Nomos, 2020),145-163.

[1339] "Motor Insurance," Insurance Europe, Accessed 31 January 2023, https://www.insuranceeurope.eu/priorities/20/motor-insurance.

[1340] "Motor Insurance," Insurance Europe, Accessed 31 January 2023, https://www.insuranceeurope.eu/priorities/20/motor-insurance.

[1341] Section 3, paragraph 3.1.6, Chapter V.

4. Some preliminary conclusions

The objective of this last chapter was to analyse the history of the many and varied theories and remedies which address the problem of ordinary objects injuring their users and how these theories might develop through the use of IoT technology in a domestic environment.

In section 2.1., I started by summarising the most important points in the history of the evolution of US products liability theories. I actually found that it was rather complex to do so, as one has to cross two groups of legal elements. On the one hand there were the different kinds of liability (tort, contractual, strict liability) and their characteristics in a specific system of common law (the US). On the other hand, I had to consider the source (or legal formant) of these kinds of liability, which is even more varied: remedies were provided by state courts, by the US Supreme Court, by national laws, by federal statutes and by authoritative doctrinal documents such as the Restatement Second and Third of Torts. As the US motto recites, "*E pluribus unum*", products liability is a unitary term which means, ultimately, a varied set of remedies which tries to strike a balance between consumers and manufacturers, guided by fairness. Unlike in the EU context where there actually is a PLD that is implemented in all MS and coexists with national liabilities that are applied when the PLD cannot be, in the US there is no such federal unitary legislation on consumer products. This, however, does not mean that all these theories are perceived, despite their differences, as a unitary part of law.

The combination of multiple sources and of different kinds of laws not only applies to products liability description, but also to technology regulation in the US and it is clear that it is also a reflection of how powers are constitutionally allocated in that country. In section 2.2., I tried to map the directions of the US approach to regulating technology. Apart from platforms, for which big changes are expected in regulation through competition law, for the IoT at the federal level there is only one bill from 2020 concerning cybersecurity, which defers the competence to standardise and establish good cybersecurity practices concerning the IoT to the NIST. There are no statutes at a national level concerning the IoT and products liability. However, California does have new cybersecurity and data privacy rules concerning connected objects (IoTs) but the statute that introduced them has several shortcomings, including the impossibility for private parties to rely on it for legal actions.

In section 2.3 I tried to analyse how the IoT was perceived by US legal scholarship. It was interesting to notice that, apart from a few exceptions, American legal scholars preferred to concentrate on robotics or AI, intended as umbrella terms that could be used almost interchangeably and that could also encompass the term IoT.

With section 3.1.1. of this chapter, I wanted to better analyse the growing corpus of judgments and FTC administrative procedures connected to domestic

IoT objects. I decided to group the cases according to the functions of the devices in domestic environments. Concerning the security of the home (smart-locks, routers and smart cameras), most of the cases actually involved the FTC, which is *de facto* becoming a regulator of data privacy and data security for domestic IoT objects by using the tools of consumer protection. Through its detailed settlement plans, which often involve concrete measures such as the implementation of cybersecurity and data privacy programs to be assessed regularly by third parties, the FTC is giving IoT manufacturers standards and good practices which they must abide by in order not to incur future FTC proceedings against them. The FTC, however, cannot do everything: for this particular field. Consumers cannot seek private action through the FTC, and the FTC monetary sanction power is limited to the circumstance where it can also enact other statutory laws granting that power, such as the COPPA[1342].

Whenever the issue of IoT object defectiveness was addressed by the courts, however, the function of the objects did not matter much as all the legal reasonings were actually quite similar, except for IoTs with healthcare functions.

The first group of cases, from *Onity* to *V-Tech,* passing through *Archer-Hays* and *Cahen*, are indeed products liability cases, as plaintiffs tried to use some of the theories cited in 2.1. (in particular implied and express merchantability warranties but also negligence), even if the products liability aspect is rarely explicitly mentioned[1343]. What makes these cases interesting is that there were also claims involving theories to prove intangible harm after data breaches. These claims were not based on products liability but on data privacy. Furthermore, said data privacy claims coexisted and often got mixed up with the ones concerning the "original" product liability claims. That is something that we might also expect to see in the EU, especially at national court level, which will likely precede the CJEU in assessing product liability claims of these products. That is why at the end of every case, I tried to imagine how that same case would have been solved by the CJEU.

Regarding the medical device cases in subsection 3.3, the products liability aspect was instead more explicit than in the previously cited judgments. There were claims based on strict liability, on negligent manufacturing and on the failure to adequately warn patients/consumers and doctors of the defects of these objects.

One element in common to all these IoT consumers object cases is the difficulty in overcoming Supreme Court precedents, such as *Clapper*, *Spokeo* and *Riegel* specifically for medical devices. Most of the times, *Clapper* and *Spokeo* were used by judges to preliminarily reject all plaintiffs' claims by a strict interpretation of Article III on the rules of Federal Civil Procedure. In fact, especially in cases where there were data breaches, it was almost impossible to prove the "in-fact" character of the injury or its immediateness. For medical devices, the same function of "filter" for the admissibility of complaints is actually the *Riegel* interpretation of section 360(k) of the MDA, which contains a pre-

[1342] Such as in the FTC *VTech* Decision and Order.
[1343] One exception is Onity where the judge refers to products liability indirectly by criticising the use that the plaintiffs had used for their arguments see specific subsection 3.1.2.

emption clause in favour of federal law and that exempts Class III device manufacturers from liability. According to this interpretation, plaintiffs must always prove the federal requirements that have been breached by the manufacturer if plaintiffs want to avoid pre-emption. Moreover, if there are state requirements (such as laws or national remedies) which also apply to medical devices, they are generally pre-empted, unless the plaintiffs plead that the state requirements are "parallel" to the FDA ones. However, the seriousness of injuries that class III devices can cause is not negligible, especially when Class III devices are manufactured negligently (they also include implantable IoT healthcare devices). If one applies constitutional jurisprudence to the letter, plaintiffs do not have any legal remedies to challenge the situation. That is why, in this kind of cases, the judge asks the plaintiffs to submit new and more accurate complaints and, by following the judge's instruction, plaintiffs may have a chance to be successful (such as in the cases leading to *Freed III* and in *Guinn I*). Alternatively, judges might consider the FDA good-manufacturing practices as federal requirements, so that the plaintiff could build a negligence or strict liability claim which is respectful of the *Riegel* doctrine.

In conclusion, it would appear that for all the non-medical IoT objects, the main challenge would be to find a solid method to demonstrate harm caused by the theft and subsequent misuse of personal information/data. This would need to be done while respecting very strict constitutional precedents such as *Clapper* and *Spokeo*. Things, however, may also start to change at state court level. As in the past, with the creation of products liability remedies, judges, not always from the Supreme Court, were observant of how society's expectations had changed over the years concerning contracts and were sympathetic with the unfairness of the situation of those people who did not have any remedy. This could happen again if we consider the effect that having personal data (or not) stolen could cause, given that our lives are lived not only in the physical world but in the online world too. The opinion of society could actually change the way judges sees these matters, even with reference to medical devices, whether they are IoT objects or not.

Regarding these last devices, the judgments analysed did not involve health data, but judges might also be prepared for cases where there is the involvement of more complex medical IoTs, or IoTs that share partly medical and partly consumer functions, such as wearables. Doubts arise about which constitutional requirements to fulfil when health and consumer functions are combined. It is not clear at the moment, but it might well be the case if the malfunctioning of the object causes physical injuries and a personal data breach. However, in that case, the more material damage (e.g., physical injuries) might take precedence and the data privacy claim would be subordinate to it.

To sum up, the analysis of US products liability theories combined with the observation of the US approach to regulating IoT technology has been insightful. It has proved to be a filter through which I could analyse cases that involved products liability issues in a more complete way. In the US, products liability

claims often combine data privacy issues. All the theories concerning data harm might help to create methods that can demonstrate one's claim, thus becoming remedies within the ensemble of the product liability ones. After all, data privacy is constitutionally a part of consumer protection, as is product liability. This process might have already started given the use made by the FTC of its consumer protection instruments in order to deal with data privacy and data security issues.

Conclusions

Conclusions 259
1. Introduction 259
2. Systematic/organisational results 259
3. Analytical results 262
4. Creative results 265
5. Conclusive remarks 268
6. Table of results 270

1. Introduction

These conclusions explain the results of the thesis' research, chapter by chapter. To carry out this task in an orderly manner, I will divide the results of the research into three main categories: systematic/organisational, analytical and creative results, which are also summarised in Table 2 at the end of the conclusions.

2. Systematic/organisational results

As explained in the introduction, Chapter II examines the functioning of the IoT from a technological and historical point of view. The origin of this technology is connected to the idea of ubiquitous computing, meaning that computing power will be omnipresent, rather than just located in certain machines, to the point that its presence in various devices may not be perceived by the public. The structure of the IoT is explained here for an audience primarily consisting of people who have studied law. Each and every part composing the IoT is explained in detail: the sensors, the gateway, the cloud, the fog and the actuators. They all concur in creating the IoT paradigm, which is based on the massive collection of human inputs (personal and non-personal data). All this produces data that is sent through the gateway to the cloud, where data is processed. In this phase, machine-learning algorithms can be applied. This is already a hint that the IoT, which unites things and the Internet, might soon be hybridised by the set of algorithms that are generally referred to as AI. Once data processing has stopped, the data is sent back through the connected object. The second set of systematic results clarified the historical smart home origin as the *non plus ultra* of luxury in the 1930s. It then also became a consequence of ubiquitous computing and sensing theories, as the IoT increasingly grew in popularity. However, today, to use the term smart home is misleading as it should be an environment that is completely connected and where all of its parts can communicate with each other and that is simply not the case. The third set of research results instead concerns the environmental unsustainability of the

current IoT model. Its main defects are that its most important data processing activities are highly centralised and carried out in the cloud where the user cannot exercise meaningful control. Furthermore, it is based on the collection of huge quantities of data, which could ultimately result in the Internet collapse. Finally, domestic IoT objects especially are renowned for their low cybersecurity levels and their reliance on rare earth materials which cannot easily be found in Europe. That is why new technologies such as Edge Computing, DLT/Blockchain and the so called Green IoT are trying to address the centralisation problem, low cybersecurity levels and the reliance on polluting materials.

In Chapter III, the systematic/organisational results mainly consist of having found all the relevant EU law that it is applicable to the home IoT. The number of laws and policies has grown over the last three years. I separated these instruments into several groups: the first is what is referred to as Data laws. It includes the GDPR, the Free Flow of Data Regulation, the E-Privacy directive, the Data Governance Act and the proposed Data Act. Then, as far as the EU consumer law *acquis*, I divided the relevant legislative acts into two sub-groups. The criterion I used was to divide the legislative acts which were drafted with the IoT as a possible object of application, such as the SDG and the DCDS, from the ones which were not. The twin directives are extremely important as they are maximum harmonization instruments regulating the contractual liability of most of the domestic IoT objects. It is also important that fundamental parts of EU consumer law, such as the Unfair Commercial Practices Directive (UCPD) and the Consumers Rights Directive (CRD) are being updated in order to make them compliant with the SDG, the DCDS, the GDPR and the “green” objectives of the New Consumer Agenda. There was also the need to introduce the PLD, which here is presented with the General Safety of Objects Directive as part of the New Approach to regulation. Moreover, in this section there are also the *ad hoc* regulation models for medical devices such as the MDD and MDR as they could apply to IoT objects with medical functions that are used in the home. In the second set of organisational results, I analysed the interferences between EU consumer law (in particular the SDG and DCDS directives) and the EU cybersecurity framework for the IoT (with the EECC and the NIS I and II directives). Finally, there was a brief explanation of how the new platform regulations, the DMA and the DSA, will indirectly apply to the home IoT. I then explained how the AI Act will in part influence the regulation of high-risk IoT applications. However, the most important thing is that with regard to private law liability, the PLD, which is in the process of being updated, will be the EU general liability system for both low- and some high-risk applications. This could be already realised by the connection that the MDR makes in Article 10(16) of the PLD.

In Chapter IV, the systematic and organisational results mainly consisted of a survey of the level of EU harmonization of the most important kinds of liability: tort/extra-contractual, strict, contractual and pre-contractual liability. The survey concerning the comparison between the levels of harmonization of the different kinds of liability generally showed that EU harmonization concerned more the remedies and behavioural duties (e.g., duties of pre-contractual information) than

the main concepts of liability, such as the validity of the contract and the causal link. The only structured liability system that has resisted the test of time is the EU strict liability model: the PLD. It is from this analysis that in the following parts of the chapter there will be an evaluation of EU competence for private law liability. This analysis will be necessary as policy makers need to select a legal basis for the new PLD, hence the principle of the conferral of competences will apply.

Also in Chapter V, there are several systematic and organisational results: they consist of a comparative analysis of different national product liability models which preceded the PLD and are partly applicable today. Thanks to these observations, it will be possible to formulate the hypothesis that the more the previous national product liability system was consumer friendly, the more the country would challenge the PLD before the CJEU, either in the context of a preliminary reference procedure or in the context of an infringement procedure. The first part of Chapter V was also used to summarise the influences and the main characteristics of the PLD. Thanks to this analysis, it was possible to connect the PLD to the model of the American Restatement Second of Torts, as they share the consumer expectation test to evaluate defectiveness, but then they differ under many other aspects. Another systematic result was to summarise the academic and judicial debate about whether the PLD had only a harmonising function (hence it was a regulatory instrument) or whether it was also a consumer protection instrument. Even if the text is not explicit, and there is an express reference to consumer protection in one of the recitals, the structure of the PLD rests on a balance between consumers' and producers' protective rules. Hence it is mainly a regulatory instrument of the Common Market. Finally, the table and the two figures (graphs) in the second section of Chapter V are systematic/organisational results *in re ipsa*. Table 1 provides a concise view of the facts, the legal questions, the AG opinions and judgments of a series of CJEU cases directly or indirectly concerning the PLD. This research was done through EURLEX, the EU law database, by inserting the keywords "product" AND "liability", from 1985 to 2022. Figure 2 shows at a glance which countries had the greatest number of PLD-related judgments before the CJEU and which kind of judgment it was (a preliminary reference procedure, an infringement procedure or a preliminary question). In the span of a few months (from March 2022, when the research was carried out, to August 2022, when the thesis was completed) one of the preliminary questions from Finland was answered and it was possible to include the very interesting *Fennia* judgment concerning the notion of the PLD producer[1344]. Figure 3 instead shows which Articles of the PLD were brought before the CJEU most frequently. The two articles most cited (alone or in combination with others) were Article 3 PLD on the concept of producer and Article 13 PLD, which instead concerned the relationship between the PLD and national liability frameworks.

In Chapter VI, there are two main systemic/organisational results. The first one concerns the synthesis of the various steps that led to the evolution of the

[1344] Reference of the *Fennia* case can be found in Chapter V, Section 2.

current US products liability framework. Under this unitary term, there are several theories that range from negligence to warranties, and from contractual liability to strict liability. The second set of organisational results concerns an analysis of the US regulation of new technologies, IoT included. As far as the IoT is concerned, the IoT Cybersecurity Improvement Act was passed at a federal level in 2020. This act enabled the NIST to commence standardising and creating good cybersecurity practices for the IoT. At the national level, on the other hand, California passed a bill in 2018 (which became effective in 2020) on privacy and connected objects (IoT). Moreover, by analysing American legal scholars' work, it was possible to understand that, apart from a few exceptions, the IoT is not an autonomous study subject, but is encompassed by the terms AI or Robotics, which are used almost interchangeably.

3. Analytical results

In Chapter II, I tried to understand why the smart home is not yet a widespread reality despite the advantages in terms of environmental sustainability and social inclusivity that could derive from its global diffusion. The lack of smart homes is mainly due to three factors. The first ones are policy factors: most of the time there was not enough computational power to sustain IoT applications for the home, the first smart home applications concerned ways of saving energy, hence they were originally connected more to electricity saving and this field of study appeared very niche and specialised (which it actually still is). The second factors are sociological: consumers were wary of their privacy, given the general low costs of this devices. This mostly concerns users who did not know much about technology. The second set of factors determining the slow diffusion of smart homes is technological. It depends on a slow and difficult roll-out of 5G technology. 5G, in fact, helps IoT objects to be faster and more accurate, especially if they have to perform actions. Moreover, the slow development of smart homes also depends on the lack of actual shared and free standards, enabling interoperability among objects.

In Chapter III, the analytical results concern, among many things, the almost insolvable issue that privacy and data protection law would always be in conflict with the current IoT model, which is based on a massive collection of personal data. The GDPR and the IoT models are antithetic, hence, it is almost certain that in cases involving IoT objects in the home, data protection will always be an issue. It was also interesting to notice that both data protection and the environment have an influence on the current indirect and informal update process of the EU consumer acquis: the UCPD and the CRD have also been updated following these trends, not only through Commission guidance documents but also formally through the Directive EU/2019/2161. The most important analytical result, however, concerns the selection of the EU private law acts that would be the most relevant for the theme of IoT home object liability. The PLD was selected because it is the document which still awaits a formal update proposal. Moreover, several legal scholars have been discussing how this

update process should be conducted and what results should be attained by its reform. More importantly, it is likely that there will be a division between high-risk and low-risk IoT objects. This is inferred by reading the EG report and also by the AI act's division of algorithms into decreasing levels of risk. Generally, domestic smart objects are considered to be low risk. Hence, whenever personal and property damages[1345] arise due to the use of these objects, the only harmonised EU legal act that could be applied is the PLD. However, if no special act concerns the liability of IoT objects (including the ones with healthcare functions) it means that high-risk IoT applications could also be subjected to the PLD. This is confirmed by the reading of Article 10(16) MDR, which redirects to the PLD for private liability. The MDR, which also considers software to be a medical device, is likely to be applied to medical IoT objects, which are generally considered high risk, or, at least, higher than simple consumer home IoT objects.

In Chapter IV, the analytical results concern society, but also changing legal vocabulary and competence issues between the EU and the MS. As far as society is concerned, the pandemic has deeply influenced how EU citizens see themselves in their home. The home is potentially people's centre of both their personal and professional lives. Moreover, there is a more widespread sensitivity to the need of combining technology and environment sustainability. If the relationship with the home has changed, people's relationship with technology has also changed with it. Consumers may be more reasonably afraid of surveillance and infringements of their privacy by their innocuous-looking voice assistants, for instance. This kind of awareness is also going to influence how we frame the liability of IoT objects. One of the main difficulties in setting up a new liability framework for a connected home relies on the complexity of the supply and value chains for IoT objects and for the domestic ones in particular. Furthermore, we will probably witness a progressive fusion of the notions of consumer, data subject and professional, at least with smart home devices. Moreover, there is no clear relationship between the Digital Single Market and the Single Market, which is very relevant for the PLD's future. Even if it is presumed that the Digital Single Market is part of the larger Single Market, there are stark differences between the two. The Single Market has always had a regulatory nature, and even if it formally respects fundamental rights, social rights such as labour rights were often compressed against the four economic freedoms, as in *Viking* and *Laval*[1346]. Conversely, the Digital Single Market has combined a human rights protection and a regulatory approach since its beginning. The latest proof of the importance of human rights in technology is demonstrated by the newly proclaimed Charter of Digital Rights.

In Chapter V, the analytical results coincide with the conclusions of the two quantitative and qualitative studies on PLD-related judgments before the CJEU. The first case study helped to identify which countries had most PLD cases before the CJEU. The country that by far had the highest number of cases was France. By combining these results with the analysis of the national liability models at the beginning of the chapter, it was possible to infer that legal systems which had a

[1345] If the conditions of Article 9 PLD are respected.
[1346] References to the cases in Chapter IV.

higher level of protection than the PLD actually tried to implement it in such a way as to make it similar to their legal tradition, as in the case of France, Denmark, Spain and Greece. On the contrary, countries which actually did not made many efforts to implement the directive actually had fewer cases, such as Germany or Italy. The UK held a strange position in this assessment: even if British PLD implementation was decidedly more favourable to producers[1347], British judges were inclined to be more lenient than expected in consumer cases involving physical injuries[1348].The second case study helped to clarify that the PLD articles that were discussed the most were Article 3 PLD, on the identity of the producer, and Article 13 PLD, on the relationship between the PLD and other national liability systems. In particular, Article 13 PLD might be the most important article of the PLD as it implicitly touches on the principle of conferral and the competence the EU has to regulate the PLD. It was observed that there is one main chronological division in Article 13 PLD-related case law. The first part of judgments went from 1995 (the year of the first PLD case) until 2004[1349]. The AG of almost all these judgments was AG Geelhoed, who maintained that the PLD was a maximum harmonization instrument, not a consumer protection one. This opinion depended on the fact that there was no consumer protection clause in the Treaties when the directive was enacted. This meant that the consumer protection clause added at a later stage in the Treaties could not be interpreted retroactively. Moreover, the entire structure of the PLD reflects the compromise between the producers' and the consumers' instances. Hence, other national liability systems could only subsist alongside the PLD if they were contractual and tort liability frameworks, and if they were special and existed prior to the PLD notification. The second part of judgments post 2004, on the other hand, concerned Article 13 PLD, hence the issue of the EU competence regulating liability indirectly. In this period, national courts made reference proceedings in order to understand whether their civil procedural laws were actually compliant with the PLD, as in *Novo Nordisk Pharma* and *Sanofi Pasteur*[1350]. The CJEU proceeded to provide inputs to national courts concerning the compatibility of their substantial and procedural rules with the PLD, the most important of which was that national procedural rules connected to the PLD had to respect the principle of equivalence and effectiveness.

In Chapter VI, the analytical results concern, on the one hand, the *de facto* IoT regulator role of the FTC and, on the other hand, the similar features of the judicial cases analysed and the contrast with the PLD judgments analysed in Chapter V. In fact, the FTC is expanding its consumer protection function to IoT domestic objects in several cases. It uses Section 5 of the FTC Act, and in particular the instruments of misrepresentation and unfair practice to issues concerning data privacy and the security of IoT objects. As for the judicial cases sharing features, the product liability claims in all the cases are never made explicit. Instead, they are referred to individually, such as negligence and strict

[1347] See *Commission v UK*, Chapter V.
[1348] See *O'Byrne* and *Sanofi Aventis*, Chapter V.
[1349] See *France v Commission I, France v Commission II, Greece v Commission, Skov Æg, Commission v Denmark, Gonzalez Sanchez*, Section 2.2, Chapter V.
[1350] See Sub-section 2.2 in Chapter V.

liability, as it is evident that they are part of the unitary concept of product liability. However, in these cases, there are also claims relating to intangible harm caused by data breaches or very probable data breaches due to proven defects in the IoT objects. The courts are very strict in applying two constitutional precedents, as in *Clapper* and *Spokeo*, to check whether the plaintiffs have legal standing, especially when plaintiffs allege that there is intangible harm involving their personal information[1351]. Most of the time, the procedural requirements of both the "in-fact" and "impendency" characters of the harm are not proven and these requirements are preliminary conditions to assessing all the other claims. Consequently, in the majority of these cases the claims are rejected because of legal standing issues. Another strict constitutional interpretation of the *Riegel* judgment concerns the pre-emption clause of Section 360k MDA. It makes it almost impossible for plaintiffs harmed by high-risk MDA Class III medical devices to prove that they sustained damage, as they need to prove an infringement of federal law, while federal law exempts class III medical device manufacturers as a default rule. Medical devices in this case also includes IoT objects with medical functions. This constitutionally strict approach is actually very similar to the results of the pre-2004 PLD judgments on application of Article 13. They concerned the relationship between the EU liability framework and national ones, just like the pre-emption issues in the US cases. The issue concerning the calculation of data harm is similar to the debate on the application of Article 82 GDPR regarding whether a violation of the GDPR must always be compensated without proof or if that there are limits to compensation in the event of violation of a GDPR rule. On this issue, Chapter V mentions the pending judgment before the CJEU and compares it with the Italian approach, which is similar to the US one, as it claims that a violation of the GDPR does not entitle a subject *per se* to compensation, as the harm that this GDPR breach caused to the plaintiffs must be proven[1352].

4. Creative results

Creative results are spread across the various chapters. In Chapter II, there is a list of methodologies to categorise the many kinds of IoT in the home. They are in part inspired by current criteria but also suggest new ones. The first one is *the new object v. updated object criterion*. Its main positive side is that it makes it easier to distinguish the many home IoT objects. For instance, the voice assistant is indeed a new domestic object, whereas a smart dishwasher is just an updated version of an existing type of object. The negative aspect is that it does not necessarily help in finding the law applicable to the smart object in the event damage occurs. The second criterion concerns the *autonomy* of the object. The different classes are made depending on the level of autonomy of each IoT object. The positive aspect of this methodology is that it creates a very complete list, but the negative aspect is that it implies that the IoT are robots, which is not necessarily true. The third criterion is based on the *EU Commission classification of consumer IoT.* The advantage here is that this classification is a good

[1351] References in Chapter VI.
[1352] See Article 9, Section 3, Chapter V.

compromise to mediate between the function of the object and the element of novelty that some of these new objects (such as voice assistants and wearables) enjoy. Moreover, the vocabulary and definitions of this document tend to be repeated in official proposals of regulations. The negative side is that it tends to be competition-law-oriented. Finally, there is *the function* criterion. Given that the IoT can have multiple different functions, the main division is objects with one main function and two or more functions. In the latter case there can be an equivalence among the functions present in the object or, alternatively, one is predominant compared to the other ones. The pro here is that this criterion is more likely to be applicable with the current set of EU laws and CJEU jurisprudence. The con is that it can be difficult to apply when assessing which function is the primary one and how it relates with the others. This will be a problem especially with IoT domestic objects that have both healthcare and consumer functions, such as wearables or exergames equipment.

In Chapter IV, the creative results concern a new way of conceiving liability, a generalisation of how the IoT supply and value chain works and, finally, an amendment to the Treaty proposal. With regard to the first result, I believe that if we want to have a more encompassing liability system that aims to integrate technology, environmental and social issues, then it is time to view liability not solely as a synonym of litigation. Rules, including liability rules, are powerful tools for businesses to assess risks, hence they are enablers for innovation. Furthermore, the presence of legal remedies actually helps consumers to trust a certain kind of technology, such as the IoT, more. As a consequence, liability rules are also trust enablers. If consumer sensitivity changes with time and it expands as to encompass the environment, then this element should be given priority when creating technology. Finally, all these further elements will make liability what it really is and will make it function in one way and not in another one. These considerations should be borne in mind and made explicit in the recitals part of the new PLD. Furthermore, from origin, liability rules are a balance between different stakeholders. Thanks to this further layer in the meaning of liability, it was relatively easy to create two generalised models of how the IoT supply and value chain is structured. In the first model, a platform or Internet search engine designs the new product (such as the voice assistant). It is then produced by a) company branches b) contractors c) a mix of a) and b). Let us bear in mind the integrated voice assistant object as an example of this model. In the second model, a producer or manufacturer that could be a) already on the market b) incumbent, with the objective of creating and marketing an IoT domestic object. This IoT object can be either a) a completely new product (e.g., a cleaning robot); b) an upgraded domestic object (a smart fridge). The second model is the most problematic due to of three factors: a) it can have several different contractors making physical or software parts of the objects; b) it may rely on a global platform or search engine also for the sake of interoperability; c) it may also require a cloud service for storage or data processing. Very often, the cloud service could be a proprietary cloud, whose owners are either the platform or the search engine with which the object should be interoperable. Finally, to solve the issue of EU competence concerning liability and to be sure that not only the internal market but also the fundamental rights protection approach

characterises the new PLD, the best solution would be to change the text of Article 114(1) TFEU and explicitly add “and the digital single market” into the text after the mention of the internal market. In this way, fundamental rights protection will be also acquired by the new PLD, which otherwise would remain just a regulatory harmonization instrument.

In section 3 of Chapter V, there are several inputs that could be used for the updating of the PLD. Inputs are given by taking into account many factors such as the insights from the previous PLD case law, the influence of the GDPR, the SDG, the DCDS and the inputs from the ELI and the representative body for EU insurance companies, Insurance Europe. They will be herein described briefly:

- Article 2 PLD: inclusion of expression “integrated” and “interconnected product”. In this way, harmonization would be easier with the SDG and the DCDS. Software, at least the one incorporated in the object, should be considered as a good and not as a service. Information should not be considered as faulty when considering a traditional object, but it could be considered defective with an IoT object under specific circumstances (e.g., when an augmented reality visor gives wrong indications on how and where to move and the consumer gets injured). The PLD should also be applicable to faulty standards and to refurbished goods.
- Article 3 PLD: a new more flexible approach to the notion of producer should be promoted given the complexity of the supply and value chain for domestic IoT. A good help to formulate this could rely on the newly rendered *Fennia* judgment, which combines Article 3 and 5 PLD and allows the consumer to sue whoever presents themselves as the producer. One could also rely on Article 82(4),(5) GDPR which establishes the principle that data controllers and processors are both liable and, if one pays and the damage is attributable also to others, MS should allow for recovery mechanisms towards the other co-debtors.
- Article 4 PLD: it is the article which concerns the burden of proof. It might just need to incorporate a combination of the rules on proof detailed by the CJEU in *Sanofi Pasteur* concerning the importance of the respect of the principles of effectiveness and equivalence while implementing the PLD through national procedural laws. There could be also the introduction of the EG’s “logging by design” principle in a presumption to make it less difficult for plaintiffs to prove the causal link.
- Article 6 PLD: the consumer expectation test should be kept in place as it is also the basis for the SDG and DCDS. There must be a way to incorporate AG Bot’s reflection on the abstract evaluation of damage for high-risk devices. Moreover, the issue of security updates should be dealt with here, maybe by adding an example of expected consumer safety measures.
- Article 7 PLD: exemptions A) and B) which concern, respectively, the responsibility of the producer of putting the product on the market and that the defect did not exist before the product was placed into circulation do not make much sense with the IoT. In fact, because of RFID tags and sensors, the producer can always have remote control over the object. Exemption 7(e) on the risk development exemption will probably stay as a counterbalance for producers, but it will be complicated how to objectively assess the state of the art, as stated by AG Tesauro, given the fast pace at which IoT technology evolves.
- Article 9 PLD: the main thing that should be considered is to find a way to harmonise, or at least to connect, Article 9 with Article 82 GDPR. At the moment, however, there is a pending judgment before the CJEU concerning the criteria, according to which immaterial damage should be compensated. Moreover, there should be an update in order to connect the new directive on representative actions to the PLD. There should also be a connection to the Environmental Liability Directive when the defect depends on polluting material or causes environmental damage.
- Article 11 PLD: the number of years for which the producer is liable should remain 10 years. Already nowadays, cases such as *Fennia, Sanofi Pasteur,* and *O’Byrne* offer guidance on the precise identification of the producer and how the time limit of liability can change when another subject substitutes the producer. Article 11 should grant better coordination with the new Articles 3, 4 and 13 PLD.
- Article 13 PLD: it is and will be the most important article of the directive. The mention of maximum harmonization should be explicit, in order to harmonise it also with the SDG and the DCDS. Moreover, it will need to integrate the rule that a national liability framework dealing with products could be maintained only if it concerns contractual or tort liability, if it concerns special categories of products and does not infringe on the rights acquired before the notification of the new directive. It will also require

integrating the MDR requisite which establishes that damage caused by IoT with medical functions (even in the home) should be compensated according to its rules, except when national liability rules are more favourable to patients (but just for medical devices).

Lastly, in Chapter VI, the creative results consist of bolder interpretations of the role of the FTC and future previsions on what kind of products liability claim we could expect in the EU regarding IoT domestic objects. As far as the FTC is concerned, the Federal Commission is becoming an indirect regulator of IoT devices, especially of the ones for the home. In fact, the FTC is creating sets of duties and standards through its settlement agreements that are *de facto* imposed on negligent manufacturers. An example of what this kind of settlements consists of is the implementation of privacy and cybersecurity programmes, which need to be assessed by third parties. Regarding comparisons and differences with legal systems, the progressive blurring of boundaries between consumer and data protection law can be noted, felt strongly in the EU and not of primary importance in the US. This is because both data privacy and product liability law could be placed within the consumer law category according to the US Constitution. We can reasonably expect, also relying on the US cases, that EU IoT cases will often involve personal and non-personal data and product liability claims at the same time if national procedural laws allow for the cumulus of different types of liability. What may be new in this context is that the cumulus could be between different sets of EU harmonised liabilities such as between the PLD and also the SDG. If the ways of calculating damage from a domestic IoT object, including the one from data breach, are not modified, the risk is that even when the damage is serious, and the complaint is not a petty one, EU plaintiffs may not be able to prove their case. A solution to this problem would be to introduce rebuttable presumptions which favour the consumer if there are no means to easily verify the functioning of the object (the logging by design principle suggested by the Expert Group on the Liability of AI). Moreover, it will also be important to apply the principles of effectiveness and equivalence when implementing national procedural laws to the new PLD, as clearly stated in *Sanofi Aventis.*

5. Conclusive remarks

This thesis was challenging in several ways: time constraints, ever-growing study material, and the lack of CJEU cases on IoT home objects are just a few of the obstacles that had to be overcome. Strangely enough, by investigating the IoT paradigm, the EU law and the concept of liability, alone and in combination with one another, it was possible to find their intersection, which focused on product liability issues, hence the decision to focus on the PLD. The PLD will be the generalised EU private law liability instrument for all kinds of technologies, domestic IoT objects included, if other special liability frameworks are not created. That is why, in order to understand where and when to change it was necessary to delve into the CJEU's PLD-related cases and analyse them first in their historical context and then speculate whether past shortcomings would coincide in all or in part with future shortcomings. For many aspects there will be an overlap with past and new problems. The issue of the PLD's

relationship with national substantive and procedural rules will likely persist. Also the doubts in identifying the producer will remain even if there seems to be an attempt to make the producer's identification process simpler for consumers while at the same time trying to be fair towards the actors of very complex supply and value chains. A more decisive tilt towards the consumer in this case has recently been made explicit by the CJEU through the *Fennia* case. To try to avoid updating the PLD for the worse, an extra effort of coordination with existing EU legal acts that are already applicable to the IoT such as the GDPR, the SDG and DCDS will be required. The comparison with the US indicates that we might expect product liability claims with data protection ones in the same judgment. Moreover, national procedural rules implementing the new PLD should also consider the procedural rule of *cumulus* of different kinds of liability. This is because today the PLD field of application could partly overlap with EU contractual liability frameworks such as the SDG, and not only with purely national liability frameworks. The comparison with the US also showed that issues on *locus standing* and pre-emption could make it extremely difficult for plaintiffs to prove their case, even when their claims are not petty. That is why it is fundamentally important that national courts especially interpret their procedural laws through the lenses of effectiveness and equivalence and that the PLD contains examples of reversible presumptions whenever the home IoT object "[…] *does not provide the safety which a person is entitled to expect*".[1353].

[1353] Article 6 PLD.

6. Table of results

Chapters	Systematic/organisational Results	Analytical Results	Creative Results
Chapter II State of the Art part I: IoT technology and the smart home	- Summary of the history of the IoT - Summary of the history of the term smart home - Summary of the structure and functioning of the IoT - List of technologies which might hybridise the IoT (Edge Computing, Blockchain, DLT, the Green Internet of Things- GIoT)	- The low rate of success and diffusion of smart homes is due to three kinds of factors: *I) policy factors* *II) sociological factors*: II) *technological factors*	-Tentative methodologies to categorise the many kinds of the IoT for the home I) T*he new object v. updated object criterion* II) *The autonomy criterion* III) The *EU Commission classification of the consumer IoT criterion.* IV) T*he function criterion*: division in one function and multifunction IoT home objects
Chapter III State of the Art part II: EU law and IoE objects in the smart home	- List of all the relevant EU private law documents mentioning the IoT and showing interconnections with this technology - The PLD is the last EU private law part of the *acquis* that is still to be updated by the EU Commission's Digital Strategy	- Clashes between IoT architecture and way of functioning especially with the GDPR - The update of the existing consumer law takes into consideration the GDPR but also tries to merge these legal concepts with environmental sustainability aspects. - Division of IoT applications into high-risk and low-risk groups. Most probably, the IoT applications for the home will be considered low risk	

		- By limiting the research field to private liability, the PLD is going to become the generalised EU legal act that is applied to both high-risk and low-risk applications (see Article 10(16) MDR)	
Chapter IV Liability in the EU and in the smart home	- The survey about the different level of harmonization of the different kinds of liability (tort, strict, pre-contractual and contractual liability) shows that harmonization concerned remedies more than definitions for the different kinds of liability analysed. However, the only structured system of liability that has resisted the test of time is the strict liability model in the EU is the PLD. - The evaluation of the EU competence for private law liability is necessary in order to fully grasp the extent of the application the future PLD.	- Deep influence of the COVID-19 pandemic on how EU citizens see themselves in their home, but also in their relationship with technology. This is also going to influence how we see liability of IoT objects - Complexity of the supply and value chain for the IoT objects and for the domestic ones in particular is going to influence the new PLD - Progressive fusion of the notions of consumer, data subject and professional, at least with smart home devices. The EU law does not yet know how to face this problem. This hybrid character will need to be borne in mind for the creation of the new PLD - Absence of a clear relationship between the Digital Single Market and the Single Market. The Single Market has always had a regulatory nature, while the Digital Single Market has combined a human rights protection and a regulatory approach since its beginning. The last proof of the importance of human rights in technology is demonstrated by the newly proclaimed Charter of Digital Rights.	- Liability connection not only to litigation, but also to risk assessment for business and to trust in technology for consumers. These considerations ought to be borne in mind when updating the PLD - Two schematised models of how domestic IoT objects are produced and marketed. This would prove useful in order to allocate liability - To solve the issue of competence and liability and be sure that not only the internal market but also the fundamental rights protection approach characterises the new PLD, the best solution would be to change the text of Article 114(1) TFEU and explicitly add the digital single market expression. In this way, fundamental rights protection will be also acquired by the new PLD which otherwise would remain only a regulatory harmonization instrument.

Chapter V Towards an updated PLD for the domestic IoE objects	- Comparative analysis of different national product liability models which preceded the PLD are partly applicable today - Synthesis of the EU PLD history, its US influence and the debate about its either regulatory or consumer protection function - Table 1 summarises the facts, the legal questions, the AG opinion and judgments of a series of cases by the CJEU directly or indirectly concerning the PLD - Figure 2 displays which countries had the greatest number of PLD or PLD-related judgments before the CJEU and which kind of judgment it was - Figure 3 shows which Articles of the PLD were brought before the CJEU the most	- The first case study helped to identify which countries had most PLD cases before the CJEU. - The second case study helped to clarify that the PLD articles most discussed were Article 3 on the identity of the producer and Article 13 PLD on the relationship between the PLD and other national liability systems. In particular, Article 13 PLD might be the most important article as it implicitly touches on the principle of conferral and the competence the EU has to regulate the PLD.	- In section 3 of the Chapter, there are several inputs that could be used for the updating of the PLD. Inputs are given by bearing in mind many factors such as : the insights from the previous PLD case law, the influence of the GDPR, the SDG, the DCDS and the inputs by the ELI and the representative body for EU insurances. They will be herein described concisely ○ Article 2 PLD: including in the new text the mention of integrated and interconnected product, so as to make it easier to be harmonised with the SDG and the DCDS; Software, at least the one incorporated in the object, should be considered as a good and not a service. PLD should also be applicable to faulty standards and to refurbished goods ○ Article 3 PLD: a new more flexible approach to identify the producer should be promoted given the complexity of the supply and value chain for domestic IoT. A good aid to formulate this could be the newly rendered *Fennia* judgment, which combines Articles 3 and 5 PLD. Article 82 GDPR which establishes the principle that data controllers and processors are both liable and if one pays and the damage is

			attributable also to others, MS should allow for recovery mechanisms towards the other co-debtors ○ Article 4 PLD: it is the article which concerns the proof. It might just need to incorporate a combination of the rules on proof detailed by the CJEU in *Sanofi Aventis* and inputs such as the one of the login by design the ones given by the Expert Group on the Liability of new technologies to make it fit for the IoT ○ Article 6 PLD: the consumer expectation test should be maintained as it also influences the SDG and DCDS; there must be a way to incorporate AG Bot's reflection on the abstract evaluation of damage for high risk devices within it; Moreover, there should be the issue of security updates dealt here, maybe by adding an example of expected consumer safety ○ Article 7 PLD: exemptions A) and B) which concern, respectively, the producer's responsibility of putting the product on the market and that the defect did not exist before the product was placed in circulation do not make any sense with the IoT. In fact, because of RFID tags and sensors the producer can always have remote control over the object. Exemption 7(e) on the risk development exemption will probably stay as a counterbalance for producers but it will be complicated how to objectively assess the

			state of the Art, as stated by AG Tesauro, given the fast pace at which IoT technology evolves ○ Article 9 PLD: the main thing that should be considered is to find a way to harmonise, or at least to connect, Article 9 with Article 82 GDPR. At the moment, however, there is a pending judgment before the CJEU concerning the criteria according to which immaterial damage should be compensated. Moreover, there should be an update in order to connect the new directive on representative actions, the MDR and the environment liability directive ○ Article 11 PLD: the number of years for which the producer is liable should stay at 10 years and should be better coordinated with the new Articles 3, 4 and 13 PLD, thanks to the principles in *O'Byrne Sanofi Pasteur* and *Fennia* ○ Article 13 PLD: it is and will be the most important article of the directive. The mention of maximum harmonization should be expressed, in order to harmonise it also with the SDG and the DCDS. It will require integrating the MDR requisite which establishes that damage caused by the IoT with medical functions (even in the home) should be compensated according to its rules, except when national liability rules are more favourable (but only for medical devices)

Chapter VI IoEd home devices in the US. Theories and cases	- Summary of the different steps that led to the evolution of the current US products liability framework - Summary of the US approach to the regulation of technology, and in particular, of platforms and IoT - Summary of the legal scholars' view on IoT technology	- The FTC's expansion of its consumer protection function to the IoT for the home in several cases. - The products liability claims in all the cases are never connected explicitly to products liability but they make reference to the theories mentioned in the first part of the chapter. However, in these cases there are also claims relating to harm created by data breaches or by the possibility of data breaches. The courts are very strict in applying two constitutional precedents such as *Clapper* and *Spokeo* when assessing whether there is any intangible harm. Most of the time, the procedural requirements of the in-fact and impendency of the harm are not proven and this is a preliminary element to assessing all the other claims. - Another strict constitutional interpretation in *Riegel* of the pre-emption clause of MDA Section 360k makes it almost impossible for plaintiffs harmed by high-risk medical devices to prove they sustained damage. Medical devices in this case also includes IoT objects with medical functions -The issue concerning the calculation of data harm is similar to the debate on the application of Article 82 GDPR in the EU	- The FTC is becoming an indirect regulator of IoT devices, especially the ones for the home. In fact, the FTC is creating sets of duties and standards through its settlement agreements which it *de facto* imposes on negligent manufacturers, such as the implementation of privacy and cybersecurity programmes, which need to be assessed by third parties - The progressive blurring between consumer and data protection law that is present in the EU when talking about IoT home device damages is not of primary importance, as both data privacy and products liability could be placed within the consumer law category. - We can reasonably expect, also relying on the US cases, that EU IoT cases will often involve personal and non-personal data and product liability claims at the same time if national procedural laws allow for the cumulus of different types of liability. - If the ways of calculating damage from a domestic IoT object, including the one from data breach, are not modified, the risk is that even when the damage is serious and the complaint is not a petty one, EU plaintiffs might not be able to prove their case. A solution to that would be to introduce legal rebuttable presumptions like the ones suggested by the

			Expert Group on Liability by also bearing in mind *Sanofi Pasteur* principles for procedural laws applying the PLD: that the principle of effectiveness should be respected.

Table 2

Latest Developments

This appendix intends to provide a brief analysis of the significant legal and policy changes that have taken place since the thesis was completed, on 31 August 2022. This appendix will exclusively focus on the legal changes involving the two proposals that are most likely to impact the private law liability framework of connected objects inside the home. On 28th September 2022, the EU Commission published two proposals concerning technology and private law liability. The first one is the proposal on the adaptation of non-contractual civil liability rules for AI[1354] and the second one concerns the proposal for the update of the PLD [1355]. In this appendix, there will be a short analysis of both proposals. Whenever relevant, there will be comparisons respectively with Chapter III, which concerned the road to the AIA (AI Act) and a legal instrument on the civil liability of AI, and Chapter V, which focused on the existing PLD structure and the perspective for a future update.

The following subparagraphs will describe the main contents of the proposal on AI civil liability (AI liability proposal, AILP) but there will be a more detailed analysis of the proposal on the update for the PLD (PLD Update, hereinafter PLDU) as it was the topic of Chapter V. Whenever necessary, there will be a comparison with previous policy and theoretical documents that were already mentioned throughout the thesis, hence in the footnotes there will be a direct reference to the chapter in which they were first explained and commented. Moreover, I will try to highlight how much these two proposals are relevant for the theme of the domestic IoT objects liability and the future IoE-powered objects.

Despite the two proposals being complementary in the field of application [1356], there are many similarities. Their legal basis is Article 114 TFEU on harmonization of internal market, hence they are not consumer protection instruments even if some of their provisions in theory favour consumers. Both of them take into consideration criteria to draft procedural rules which should favour consumers when it is difficult to prove one of the elements of non-contractual or strict liability regimes every time AI-powered or IoT technologies are involved[1357]. The two directives both rely on sets of definitions which try to connect different legislative acts or proposals (such as the DSA, the DGA and the Trade Secrets Directive[1358]). One main difference is that the AILP might appear more abstract

[1354] "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), Brussels, 28.9.2022 COM(2022) 496 final 2022/0303 (COD)," European Commission, Accessed 31 January 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_5807.

[1355] "Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on liability for defective products, Brussels, 28.9.2022 COM(2022) 495 final 2022/0302 (COD)," EU Commission, Accessed 31 January 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_5807.

[1356] Article 1(3)(b) of AILP in fact expressly excludes from its field of application the issues that are covered by the PLDU.

[1357] See Articles 3 and 4 AILP and 8 and 9 PLDU.

[1358] "Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (Text with EEA relevance) *OJ L 157,* 15.6.2016, p. 1–18," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0943.

as the key definitions of fault and negligence are mainly left to MS laws. However, the only explicit definition of a constitutive part of non-contractual liability, duty of care, is explained in Article 2(9) AILP and it coincides only with "*a required standard of conduct, set by national or Union law, in order to avoid damage to legal interests recognised at national or Union law level, including life, physical integrity, property and the protection of fundamental rights*"[1359]. This is relevant as in the MS there are different definitions and declinations of the duty of care and having a European duty of care that is defined conceptually is a big step towards further harmonization of private law liability systems.

Moreover, both proposals concern the subjects that can receive compensation. According to Article 2(6)(a)(b)(c) AILP and Article 5 PLDU, it is not only the person who endured the damage that has a right to compensation but also the person "[…] *who has succeeded to or has been subrogated to the right of an injured person by virtue of law or contract; or* […] *is acting on behalf of one or more injured persons, in accordance with Union or national law*"[1360]. This is extremely important as both provisions allow insurance companies as subjects to become authorised representatives of the claimant explicitly under EU law and also collective procedural remedies.

1. The AI Civil Liability Proposal (AILP)

The AI liability proposal (AILP) is the final step of a path started from the Trustworthy AI Guidelines to the Expert Group on the Liability of AI and new Technologies report, whose founding concepts were already accepted by the European Parliament resolution of October 2020[1361], and were partly translated into the AI Act (AIA) proposal, which implements the Expert Group's main idea of dividing algorithms according to the levels of risk they involve for fundamental rights.

To start the analysis, it is important to notice a connection between the AIA (AI Act proposal) and the AILP. Conceptually, the main link with the previous preparatory documents and the AILP is the persisting distinction between high-risk AI systems and low-risk AI systems. This distinction is relevant because high-risk algorithms are the main target of the regulation according to Article 1(1) AILP. Article 1 AILP is also clear in outlining what is outside the application of the proposal. Article 1(3) AILP specifies that the rules concerning transport[1362], the application of the PLD[1363], the liability exemptions of the DSA concerning platforms and search engines[1364] and the "[…] *national rules determining which party has the burden of proof, which degree of certainty is required as regards the standard of proof, or how fault is defined*" that are different from the evidence

[1359] Article 2(9) AILP.
[1360] Article 2(6)(a)(b)(c) AILP and Article 5 PLDU
[1361] Both of these documents are discussed in depth in Chapter III.
[1362] 1(3)(a) AILP.
[1363] 1(3)(b) AILP.
[1364] 1(3)(c) AILP.

disclosure and legal assumptions in Articles 3 and 4 AILP are excluded from the field of application of the same AILP.

Regarding the connections between the AIA and the AILP, not only are they conceptual (e.g., high-risk v. low-risk) but also on the definitions level. The definitions aspect is particularly evident in Article 2 AILP. This provision makes a direct reference to the AIA as far as four important words are concerned. These terms are, respectively, "AI system", "high-risk AI system", "provider" and "user"[1365].

Regarding the main characteristics and features of the proposal, from a EU constitutional point of view the AILP legal basis is -unsurprisingly- Article 114 TFEU. In the explanatory memorandum, it is stated that one of the main functions of this proposal is to "[…] *have a positive impact of 5 to 7 % on the production value of relevant cross-border trade as compared to the baseline scenario*"[1366], but also to make access to effective justice systems possible and also to help in reaching the SDG goals, as AI supposedly makes several production processes less wasteful[1367].

It is important to point out that, as well as the actual PLD, the AILP does not clearly state whether it is a maximum or minimum harmonization directive. The fact that there is no mention of what fault consists of seems to indicate that it is a minimum harmonization directive, at first. To support this claim concerning the AILP minimum harmonization character is Article 1(4) AILP which states that "[…] *Member States may adopt or maintain national rules that are more favourable for claimants to substantiate a non-contractual civil law claim for damages caused by an AI system, provided such rules are compatible with Union law*." [1368] Another example is in Article 2 AILP: there are two new important definitions of claim for damages[1369] and claimant[1370]. The definition of claim for damages is rather general and makes reference to the national legal system to define what is "non-contractual" and "fault-based" but there is an innovative addition to that. Article 2(5) AILP regarding the claim for damages can only be applied whenever damage is "[…] *caused by an output of an AI system or the failure of such a system to produce an output where such an output should have been produced.*"[1371] In addition to that, the definition of claimant is still general but quite innovative in its structure. In the AILP, the claimant is not only the person who is injured by an AI system, but also a subject who might be surrogated in the rights of the victim of the damage[1372] or is acting on behalf of two or more people[1373]. It is quite relevant that a collective and transnational dimension has been added to the proposal. As explained in the *Lloyds* case in the UK Supreme Court (Chapter V), technological damages often have a collective dimension and

[1365] See Articles 2(1)(2)(3)(4) AILP which refer respectively to Articles 3(1) AIA, 6 AIA, 3(2) and (3) AIA..
[1366] AILP explanatory memorandum, 4.
[1367] AILP explanatory memorandum, 4.
[1368] Article 1(4) AILP.
[1369] Article 2(5) AILP.
[1370] Article 2(6)(a)(b)(c) AILP.
[1371] Article 2(5) AILP.
[1372] 2(6)(b) AILP.
[1373] 2(6)(c) AILP.

national procedural instruments, even the ones for groups of people, may at times not be suited for this kind of damages[1374]. These innovative aspects of otherwise general and MS-reliant definitions might hint that application of the AILP could be more extensive and more harmonised than thought. This would hardly be a new thing in the application of EU law, as already happened with the PLD. It seems highly likely that to ensure the relevance of the AILP, CJEU judges especially would interpret it more as a maximum harmonization directive, as also Article 1(4) AILP contains a potential basis for the EU to assess the compatibility of national liability systems. In its final clause, it states that national systems, although different, need to be respectful of EU law when regulating civil liability of AI.

The true turning points of the whole proposal are Articles 3 and 4 AILP. By relying on the considerations regarding the intrinsic opacity, complexity, autonomy and "data-drivenness" characters of AI powered technologies[1375], the Expert Group on the Liability of AI and New Technologies had suggested some measures to give claimants a fairer chance to prove that an AI system had caused damage. As discussed in Chapter III and V, among the main suggestions of the Expert Group were the right to access the logs of the device easily (the right of logging by design)[1376], and a series of legal presumptions in favour of the claimant whenever the AI-powered object did not respect relevant and sector-specific safety rules (cybersecurity ones included). Moreover, there was also a presumption concerning causation, and/or fault or the existence of the defect that would be in favour of the claimant [1377]. Also [26] of the same report introduced the principle of the alleviation of the burden of proof by balancing out different interests[1378]. The idea of allowing consumers to rely on legal presumptions in the event it is difficult to prove any of the elements that traditionally concern non-contractual liability, such as fault, the duty of care, negligence and the causal link is at the core of both Articles 3 and 4 AILP, but they concern different procedural phases of a trial for AI-induced damage.

Article 3 AILP focuses mainly on the disclosure of evidence, a remedy that can be used when constructing the claimant's case. In fact, Article 3(1) AILP sets out the principle that national courts must have the means to disclose relevant evidence about a specific high-risk AI system that could be the cause of the

[1374] Briefly, the claimant had started a putative class action because Google had tracked its IOS devices' action through a spy cookie and alleged that thousands of people had experienced the same kind of damage. The Supreme Court stated that it was not proven how the claimant could demonstrate that his personal damage was the same as other people's and why. Read more in Chapter V, 3.1.6. Future Article 9 PLD.

[1375] Expert Group on Liability of AI and New Technologies, 5.

[1376] [20] Expert group report.

[1377] [24] Expert group report.

[1378] More specifically, "[…] *(a) the likelihood that the technology at least contributed to the harm;*
(b) the likelihood that the harm was caused either by the technology or by some other cause within the same sphere;
(c) the risk of a known defect within the technology, even though its actual causal impact is not self-evident;
(d) the degree of ex-post traceability and intelligibility of processes within the technology that may have contributed to the cause (informational asymmetry);
(e) the degree of ex-post accessibility and comprehensibility of data collected and generated by the technology
(f) the kind and degree of harm potentially and actually caused." [26] Expert Group report

damage[1379]. This action from the courts is only permitted if the claimants have unsuccessfully tried to gain access to the high-risk algorithm way of functioning[1380] and that they "[…] *present facts and evidence sufficient to support the **plausibility** of a claim for damages*"[1381]. The mention of the term plausibility is not only an AILP characteristic. In fact, it also appears in the other liability directive, the PLDU, in "twin" Article 8 PLDU. However, there are no indicators on how to evaluate this plausibility[1382]. Arguably, plausibility could be assimilated into the concept of *fumus boni iuris* in some of the MS. What the AILP is clear about is the need to balance these elements in favour of the claimant in a way that safeguards the IP rights, know-how or trade secrets of the high-risk algorithm creator and which may be revealed during the disclosure of evidence[1383]. This exercise in balancing must be done by evaluating whether the disclosure is necessary and proportionate to the damage endured and the likelihood of its connection to the high-risk performing algorithm[1384]. At the end, Article 3(5) AILP adds a further presumption that is, theoretically, an advantage for the claimant: whenever a court issues an order to disclose evidence in the ways and forms allowed by the previous paragraphs and the addressee refuses or fails to comply, the national court is allowed to presume non-compliance with a relevant duty of care such as the ones present in the AIA that are cited by the following Article 4. However, all the presumptions described in the article are rebuttable.

Article 4 AILP concerns the presumption of the causality link and is divided into two parts. The first one has a general character, and it explains how and when the presumption concerning the causality link between the defendant's fault and the output produced by the AI system, or the failure of the AI system to produce an output, is applicable[1385]. In particular, three cumulative conditions must be fulfilled by the claimant. The first one[1386] is when "[…] *the claimant has demonstrated or the court has presumed, pursuant to Article 3(5), the fault of the defendant, or of a person for whose behaviour the defendant is responsible, consisting of the non-compliance with a duty of care laid down in European Union or national law directly intended to protect against the damage that occurred*"[1387]. The second condition is respected when, it is likely that "[…] *the fault influenced the output of the AI system or the failure of the AI system to produce an output*"[1388]. The last condition is that the claimant successfully demonstrated that the output produced by the AI system or the failure of the AI system to produce an output gave rise to the damage[1389].

[1379] 3(1) AILP.
[1380] Access could be denied by either a provider or subject to the obligations of a provider according to Articles 24 or 28(1) AIA, but also another user. Article 3(1),(2) AILP.
[1381] Article 3(1) AILP, emphasis added.
[1382] Even Recital 17 AILP mentions plausibility but does not define it further.
[1383] Article 3(4) AILP.
[1384] Article 3(4) AILP.
[1385] Article 4(1) AILP.
[1386] Article 4(1)(a) AILP.
[1387] Article 4(1)(a) AILP.
[1388] Article 4(1)(b) AILP.
[1389] Article 4(1)(c) AILP.

The second part of Article 4 AILP takes into consideration specific requirements for high-risk AI systems and the different kinds of subjects involved in their faulty implementation. One of the conditions of Article 4(1) AILP may be automatically satisfied in the event of non-compliance with a certain set of AIA requirements by a selected group of subjects. What really matters is the kind of subject that is considered as the potential defendant. In fact, Article 4(2) AILP is applicable only to those algorithms that are subject to the requirements in Chapters 2 and 3 of Title III of the AI Act, which concern the requirements for high-risk systems, and the obligations of providers, or people subordinate to the providers under articles from 24 to 28 AIA. In such cases, the first of the three conditions of Article 4 AILP outlined above is satisfied if the claimant demonstrates those subjects' non-compliance with the requirements of the AIA that in this context are *de facto* assimilated to duties of care. For instance, to create a high-risk AI system which does not respect the transparency requirements set out in Article 13 AIA could help consumers to presume that the AI-system caused the damage that actually ensued. Article 4(3) AILP, on the other hand, concerns a different set of subjects (users) and the non-compliance with the requirements laid down in chapters 2 and 3 of Title III of the AIA. If these two sub-conditions are satisfied *ratione materiae* and *personae*, the condition of 4(1) (a) AILP (the first one leading to the presumption of the causality link) "*shall be met when the claimant proves that the user:*

(a) did not comply with its obligations to use or monitor the AI system in accordance with the accompanying instructions of use or, where appropriate, suspend or interrupt its use pursuant to [Article 29 of the AI Act]; or

(b) exposed the AI system to input data under its control which is not relevant in view of the system's intended purpose pursuant to [Article 29(3) of the Act]"[1390].

Finally, although the entire directive proposal addresses mainly high-risk AI systems, Article 4 makes it possible for judges to also apply the presumption of Article 4(1) AILP to low-risk AI systems "[…] *where the national court considers it excessively difficult for the claimant to prove the causal link*"[1391]. It appears that this should be a residual legal solution for those low-risk AI algorithms that, for some reason, are not included in the field of application of the PLDU (see infra). Before concluding that none of the presumptions are non-rebuttable[1392], there is a last residual scenario that is addressed by Article 4(6) AILP. If a defendant caused damage by using an algorithm in the context of a non-professional activity, the judge could apply the legal presumption on the causality link of Article 4(1) AILP only if "[…] *the defendant materially interfered with the conditions of the operation of the AI system or if the defendant was required and able to determine the conditions of operation of the AI system and failed to do so*"[1393].

At the present time, the proposal on AI liability must still undergo all the phases of the ordinary legislative procedure and it is impossible to know whether

[1390] Article 4(3) AILP.
[1391] Article 4(5) AILP.
[1392] Article 4(7) AILP.
[1393] Article 4(7) AILP.

the finally approved text will be the same as the one described to date. However, it is important to observe that the mechanisms of legal presumptions and substantial procedural principles favourable to consumers finally made in the AILP proposal draft from the 2019 Expert Group report. The disclosure of evidence in Article 3 AILP is one of the most relevant aspects together with Article 4 AILP. However, the connection between the first part of Article 4(1) AILP, which clarifies the rule to apply the causality link presumption, with other specific elements (such as the requirements of the AIA and the kind of defendant involved) is not so easily comprehensible, even though its function is to help consumers prove their claim. This complexity and the fact that judges need to evaluate the proportionality and necessity for the disclosure of evidence in Article 3(4) AILP make this instrument a market integration instrument as the competing interests of AI-systems creators and consumers are taken into account. This proposal appears to be of minimum harmonization, as the concept of fault and legal actions are still controlled by the states. However, if there is the political will to transform it into an instrument that is able to truly harmonise the field of AI-induced damages, one can easily remember that the CJEU established that the PLD was a maximum harmonization directive *de facto* by counting on the fact that there was no explicit mention of minimum harmonization. I believe it is likely that, whatever the final text will be, the CJEU would prefer a maximum harmonization approach for these kinds of damages, which will be in the majority transnational. As far as the relevance for the IoT (soon to be IoE) domestic objects, the AILP will be applicable only if the algorithms that are employed in the cloud for the functioning of these objects could be labelled as high-risk. For the low-risk AI applications, hence for the most part of contemporary domestic IoT objects, it will be the PLDU proposal that is likely to be the most applied EU legislative act as far as strict liability is concerned. This will be better explained in the following subsection.

2. The PLD Update (PLDU)

The PLDU is a rich proposal which takes into consideration a considerable number of the policy insights discussed in Chapter V, and the latest ELI document on the PLD which I learned of just after the completion of the thesis last 31 August 2022 and that I will refer to with the terms ELI draft or ELI PLD draft[1394]. In this subsection there will be an analysis of the proposal structure and, whenever possible, I will highlight similarities and differences with the ELI documents concerning the update of the PLD and Chapter V final policy suggestions. The PLDU in fact will be essential in creating a private law liability framework for domestic IoT (future IoE) objects. As explained through Chapters III and V, the PLD will be applied to connected objects that could contain integrated or stand-alone software whose way of functioning is considered low-risk, according to the

[1394] ELI Draft of a Revised Product Liability Directive," ELI Website, Accessed 31 January 2023, https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Draft_of_a_Revised_Product_Liability_Directive.pdf.

AI act (AIA), such as IoT-powered domestic objects. Hence, it is of the utmost importance to understand what the changes introduced by the PLDU will be, because it will be applied to the same category of domestic connected IoT objects and, in perspective, to the future IoE objects for the home.

The PLDU proposal is divided into four chapters. The first one concerns the so called "general provisions". It includes articles on the subject matter, the scope, the level of harmonization and important definitions for the directive[1395]. Unlike Article 1 PLD, which lays down the principle of a producer's liability, Article 1 PLDU instead mentions the liability of "economic operators". That appears to be a relevant systematic change, as already in article 4 PLDU the word producer is not mentioned but is substituted by the word manufacturer[1396]. By reading other definitions from Article 4 PLDU's list of subjects, including the ones of authorised representative[1397] and importer[1398], it is clear that "economic operators" may be the more interesting one as it means "*the manufacturer of a product or component, the provider of a related service, the authorised representative, the importer, the fulfilment service provider or the distributor*"[1399]. Therefore, it is a collective name that refers – theoretically - to any subject involved in the IoT product and value chain. The rationale under this series of old (such as importer) and new subjects (such as the fulfilment service provider and, at some conditions, online platforms[1400]) is most probably dictated by the evident complexity of the IoT value and supply chain explained in Chapter IV and the need to allocate liability more fairly along the production chain.

Nevertheless, the CJEU has recently been leaning towards the consumer as far as the identification of the true producer is concerned. In its recent *Fennia v Philips* case[1401], it pointed out that whenever consumers are undecided about which subject is the producer, they can sue the one that would appear to be one, as Article 3 and 5 PLD take into consideration the case of the plurality of producers and how to regulate their relationship after one of them has paid for compensation. It will be interesting to balance this with the need for economic operators to have some order and priority in finding who must be held liable when the actual manufacturer is located outside the EU[1402], which seems to be the rationale of Article 7 PLDU on the liability of economic operators. Moreover, this is also relevant for EU businesses as they need to understand how to allocate risks. In particular, by following the ELI draft of the PLD, the Commission has created a more refined mechanism to identify who needs to pay for compensation in Article 7 PLDU, as is already the case in the MDR[1403].

[1395] They are respectively Articles 1, 2, 3 and 4 PLDU.
[1396] Article 4(11) PLDU.
[1397] Article 4(12) PLDU.
[1398] Article 4(13) PLDU.
[1399] Article 4(16) PLDU. The term economic operator can also be found in Article 2(35) MDR.
[1400] Article 4(17) PLDU.
[1401] C- 264/21
[1402] Which is definitely the case as far as technological objects like domestic IoT are concerned and it is also one of the motivations underpinning this proposal. See Explanatory Memorandum of the PLDU p.2
[1403] See Article 2(30),(31)(32)(33) (34)(35) MDR. In particular, Article 7 PLDU mechanism presents some similarities with Article 16 MDR.

One of the most innovative and long-awaited measures of the proposal concerns the introduction of software, both integrated in the device and in a stand-alone context as a product[1404]. This idea that electricity and software are products also enriched the very definition of component[1405]. More importantly, it means that the differences in the regimes of the circulation of goods and services provided by the Treaties and by the MS national rules will not be applicable to the product liability claims concerning low-risk AI applications, such as domestic IoT objects, because software, data and related services will only be considered as goods. Article 4 PLDU contains no particular effort to harmonise the PLDU with the vocabulary that is already known and applied in EU law through the SDG and DCDS, as was instead suggested at the end of Chapter V and in the ELI Draft of the PLD[1406]. It is more of an indirect reference to the same kinds of connected objects instead of a specific reference to definitions such as for the AIA and the AILP. An example of this allusion to the connection with the SDG and DCDS is the term "related service"[1407], which highlights the "interconnectedness" of software with products[1408].

Chapter II of the PLDU instead concerns the instructions on the right to compensation, the concept of defectiveness, the list of liable economic operators and the instructions that mirror the AILP on the disclosure of evidence and the burden of proof. Lastly, it ends with a set of the old and partially new exemptions from liability rules and exceptions to these ones[1409].

The product liability demonstration mechanism is the same as the one in the previous PLD. Article 9(1) PLDU, like Article 4 PLD, mentions that the consumer must prove the defectiveness of the product, the damage suffered and the causal link between defectiveness and damage. What the PLDU tries to change is the meaning of some of the elements of Article 4 PLD, such as the concepts of defectiveness and damage [1410], or to introduce mechanisms that can help prove the causality link in some circumstances[1411] .

As was also suggested in several ELI position papers and in Section III of Chapter V of this thesis, the concept of defectiveness required an update. With regard to defectiveness, it is important to point out that the main criterion to judge defectiveness (the safety that a person can legitimately expect from Article 6 PLD) is mostly same in the new Article 6(1) PLDU, but there is a word change whose extent is still unclear. The term "public at large" as the point of reference for the level of safety to be expected has substituted "person" as stated in Article 6 PLD. It is uncertain whether the Commission wanted to highlight the often-collective dimension of damages that could specifically affect smart object owners. Article 6(2) PLDU adds some examples on how to evaluate the

[1404] Article 4 (1) PLDU.
[1405] Article 4(3) PLDU.
[1406] ELI Draft, executive summary, 7.
[1407] Article 4(4) PLDU.
[1408] See the definition of goods in Article 2(5)(b) SDG and 2(1),(2),(3) DCDS on digital content, digital service and goods with digital elements.
[1409] They are respectively Articles 5,6,7,8, 9,10 PLDU.
[1410] Such with the new Article 6 and damage in Article 2(6) (a),(b),(c) PLDU.
[1411] Such as with the new Article 8 and 9) PLDU.

defectiveness of the product and many of the options refer implicitly to low-risk connected objects such as domestic IoT items. An example of the connection to smart objects is that among the examples of "defectiveness" Article 6 PLDU (c) mentions the "*effect on the product of any ability to continue to learn after deployment*" which makes reference to automated-learning algorithms. Furthermore, there is a specific connection with the cybersecurity legislation in Article 6(1)(g) PLDU which makes the need to respect the "*safety relevant cyber security requirements*" explicit. Together with the need to respect the interventions of specialized national and EU authorities on the safety of technological products that could be found at Article 6(1)(f) PLDU, domestic smart objects economic operators will need to consider many more sources (of a technical and administrative kind) in order to fulfil an implicit duty of care which more specifically concerns the obligation to provide a safe IoT connected object for the home, for example. This raises doubts as to whether small companies such as start-ups will ever be able to be up-to-date with all these issues. On the contrary, international big companies producing IoT for the home will be able to better manage further investments in research and compliance that the PLDU will require of them. It will be more difficult to interpret letter h) of the same article, as it states that defectiveness can be derived from "*the specific expectations of the end-users for whom the product is intended"*[1412]. The answer to the question of what the end-users' expectations are would be a national and CJEU judges' task.

As far as the kinds of damage that could be compensated, the PLDU includes personal injury and death, damage to property, but there is no connection or reference to either damage to personal data or to pure economic loss. This perspective, meaning the exclusion of personal data damages from the PLDU was advocated mainly by the Insurance Europe group report[1413]. Article 2(6) PLDU limits damage to the "material consequences" that can happen to a physical person and for the first time it clarifies that it also covers "*medically recognised harm to psychological health*". This was not explicit in Article 9 PLD and only through the *Veedfald* judgment[1414] was it possible to also cover immaterial damage, provided that this was also allowed by national law. However, Article 2(6)(c) PLDU includes "*loss or corruption of data that is not used exclusively for professional purposes*". It is interesting that data is defined by taking the newly approved, and well-defined DGA categories into consideration and not those laid out in the GDPR[1415]. With regard to property damage, it is interesting to notice that there is no monetary threshold as there was in Article 9(b)(i) (ii) of the former PLD, which is an element that could see an increase in the number of cases that will require application of the PLDU, even more in countries where the PLD was not employed unless necessary, as in Germany for example[1416].

[1412] Article 6(1)(h) PLDU.
[1413] See Chapter V.
[1414] See Chapter V.
[1415] According to Article 2 (1) data "means any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audiovisual recording".
[1416] See Chapter V, section II.

Like the AILP, the PLDU also has rules concerning civil procedure. Or, rather, the PLDU has rules concerning what the MS are allowed to do with the procedural principles set out in the directive. The main difference is that while the AILP appears to be a minimum harmonization directive, the PLDU states that the product liability rules are ones of maximum harmonization in Article 3 PLDU [1417], as the course of action suggested at the end of Chapter V, and unlike what was stated in the ELI PLD Draft that contemplated more freedom for the MS in this respect[1418]. The advantage of making the maximum harmonization element explicit is actually allowing the latest CJEU jurisprudence on the application and harmonization of procedural rules involving the application of the PLD to be used. This issue was widely discussed in Chapter V. This is clear when reading Articles 8 and 9 PLDU concerning the disclosure of evidence and burden of proof which have a very similar mechanism to Article 3 and 4 AILP. The reference to the criteria of necessity and proportionality is similar to the one of effectiveness and efficiency suggested by AG Bobek and AG Szpunar in *Novo Nordisk Pharma* and *Sanofi*[1419]. Article 8 PLDU is drafted as a copy of Article 3 AILP. Claimants will need to demonstrate the plausibility of the claim to compensation. As in Article 3 AILP, Article 8(3) PLDU will require claimants to demonstrate the plausibility of their claim through facts and evidence. MS laws will need to balance this disclosure to what is necessary and proportionate[1420]. In order to do that it will be necessary to consider the legitimate interest of all parties, including third parties, with special reference to trade secrets[1421]. If the defendant fails to disclose evidence when asked by a national court, then Article 9(1)(a) makes it possible to imply defectiveness of the product. Although very clear as a principle, the balance between the concerned economic operator's IP rights and the consumer's access requests is not easy to strike. A national application of this rule might entail an even wider fragmentation of the Digital Single Market as not only will there be different national procedural rules to apply this principle but also there will be the judges' different views. Concerning this last element, it is unlikely that judges will analyse and study these cases on their own. Most probably, they will require a third-party impartial expert which will inevitably also shape their decision-making process. Consequently, this will impact on MS systems of constitutional inner checks and balances systems as the magistrate's opinion is not completely their own. Nevertheless, the over-reliance on experts in technical matters by judges is something that is already happening[1422]. As a consequence, it will increase the proceedings costs and, ultimately, it will impact the role and authority of courts as they will tend to apply third party experts' opinions to product

[1417] Article 3 PLDU.
[1418] Article 4 ELI PLD draft.
[1419] References in Chapter V.
[1420] Article 8(3) PLDU
[1421] "Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (Text with EEA relevance)
OJ L 157, 15.6.2016, p. 1–18," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0943.
[1422] Alberto Alemanno, "Science & EU Risk Regulation: The Role of Experts in Decision-Making and Judicial Review. EUROPEAN RISK GOVERANANCE - ITS SCIENCE, ITS INCLUSIVENESS AND ITS EFFECTIVENESS, Connex Report Series No. 6, E. Vos, ed., February 2008", SSRN (2014). Accessed 31 January 2023, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1007401.

liability cases involving domestic IoT as well. This is bound to happen even if, formally, judges could always refuse an authorised third opinion and decide on their own, although it would be more difficult to motivate their decisions.

The second article concerning procedural law principles is Article 9 PLDU. It is a complex article that in its first paragraph outlines the elements that must be proved when asking for product liability compensation. The three elements to prove are no different from the ones in Article 4 PLD. This means that the claimant must still prove the defectiveness[1423], the damage suffered[1424] and the causal link. As IoT objects, even the ones for the home, also have complex ways of functioning that are difficult to understand, the PLDU introduces some rebuttable presumptions concerning the burden of proof. Unlike in Article 4(2) AILP, where the conditions concerning the causality link are cumulative, in Article 9(2) PLD the three conditions concern a different aspect of liability (defectiveness) and are not cumulative. In fact, if the manufacturer does not respect the obligations of Article 9(2) PLDU which include: *"(a) the failure to comply with the obligation to disclose relevant evidence at its disposal pursuant to Article 8(1) PLDU*, [or the fact that] *(b) the claimant successfully proved that the product is non-compliant with mandatory safety requirements or that (c) the claimant establishes that the damage was caused by an obvious malfunction of the product during normal use or under ordinary circumstances*."[1425] Concerning the causality link instead, Article 9(3) PLDU states that it will be presumed, "*where it has been established that the product is defective and the damage caused is of a kind typically consistent with the defect in question*". Although the content of this part of the article is clear intuitively, it will not be easy to apply. Judges and consumers will need to probably take into consideration the ENISA's annual threat landscape report and keep track of the national product safety and cybersecurity authorities' documents to motivate the application of this presumption. In the most difficult cases, Article 9(4) PLDU provides the claimant with a presumption in its favour whenever *"(a) the product contributed to the damage; and (b) it is likely that the product was defective or that its defectiveness is a likely cause of the damage, or both.*"

One innovation in this section is that, indirectly, the PLDU gives the possibility to insurance companies to play a more active role also with regard to damages created by connected consumer objects, as stated in Article 5(2)(a),(b) PLDU[1426] as they will be able to be subrogated in the consumers role against the economic operator. However, it is still not clear how the MS will implement this order and whether there will be a future harmonization of insurance contracts for low-risk AI-powered objects such as domestic IoT devices. What is likely, however, is that the economic operators involved in these processes will be interested in stipulating insurance contracts protecting them from the most

[1423] Criteria for establishing defectiveness are specified in Article 6 PLDU.
[1424] Article 2(6) PLDU.
[1425] This Article structure took inspiration by the latest ELI PLD draft Article 9.
[1426] Article 5(2) (a)(b) recites "*Member States shall ensure that claims for compensation pursuant to paragraph 1 may also be brought by:*
(a) a person that succeeded, or was subrogated, to the right of the injured person by virtue of law or contract; or
(b) a person acting on behalf of one or more injured persons in accordance with Union or national law".

serious risks created by their IoT products for the home. As an example, let us consider a kind of stand-alone software, such as a successful downloadable application. Under the PLDU, the application is a product. If this product causes damage (for instance to data) then a potentially very high number of people might ask for compensation on the basis of the PLDU, even through collective actions. To avoid bankruptcy, an *ad hoc* insurance contract concerning product liability would appear to be the best option for the concerned economic operator.

It is also worth mentioning that the new article on how to allocate liability is not included among the initial ones: it is no longer Article 3 PLD but Article 7 PLDU. The title of the latter, "liability of economic operators" has a general tone, but the paragraph maintains that the manufacturer is the primary subject liable towards the consumer or the manufacturer of a defective component[1427]. The subjects that could be held liable when the manufacturer is established outside the EU are the importer and the authorised representative[1428]. If also the importer and authorised representative are not EU-based, it will be the fulfilment service provider who will be held liable[1429]. Moreover, it is important to highlight that if the product is modified (it is most likely a reference to refurbished products, as hoped by the ELI earlier documents and from Chapter V conclusions) then the person responsible for the modification should be held liable[1430]. Article 7(5) PLDU envisages the hypothesis that the manufacturer either cannot be identified, or, whenever it is based outside the European Union and an economic operator such as an importer or authorised representative cannot be identified, each distributor of the product could be held liable "*if (a) the claimant makes a request to that distributor to identify the economic operator or the person who supplied the distributor with the product; and (b) the distributor fails to identify the economic operator or the person who supplied the distributor with the product within 1 month of receiving the request*."[1431] This part of the Article amends what is now Article 3(3) PLD, which does not provide any clear framework on how to communicate the identity of the producer to the consumer. This was the main problem at the heart of the vaccine case *O'Byrne,* where there also was the problem of potential time-barring of the claimant and, more generally, this issue was crucial in all the judgments concerning the role of Article 3 PLD and its applicability to the supplier such as *Commission v. France I, Commission v. Greece, Gonzalez Sanchez* and *Skov Æg*. Interestingly, Article 7(5) PLDU is also applicable "*to any provider of an online platform that allows consumers to conclude distance contracts with traders and that is not a manufacturer, importer or distributor*" provided that the conditions in Article 6(3) of the DSA are satisfied. This is a turning point as what most of the digital or non-digital content consumers are interested in is through platforms that are accessible through the IoT object. However, if one must follow the precise order set by Article 7 PLDU, online platforms are not the first economic operators that a consumer could ask for compensation because, as the distributors in Article 7(5) PLDU, they are the

[1427] Article 7(1) PLDU.
[1428] 7(2) PLDU.
[1429] 7(3) PLDU.
[1430] 7(4) PLDU.
[1431] 7(5) PLDU.

consumers' last resort according to Article 7(6) PLDU. This should be the rule even though online platforms might be the first point of contact with the manufacturer and, in certain cases, they do appear as the manufacturer itself.

With regard to the liability exemptions, contrary to what is expected at the end of Chapter V and in the ELI draft of the PLD[1432], they are not fewer than the current ones but actually more. Article 10 PLDU maintains the previous rules by changing the language of the different exemption options[1433] or by redrafting them, and by adding a specific exemption for refurbished products[1434]. As was discussed at the end of Chapter V, it was unlikely that the Commission took away the risk development exception, which is codified with the same letter that it has in the PLD[1435]. I still maintain that there could be discussions concerning the AG Tesauro's interpretation of what the state of the art for technology today is by following his "objective" criterion developed in *Commission v. UK* many years ago. As far as more consumer-friendly provisions are concerned, Article 10(2) PLDU states that the exemption in Article 10(1)(c), which exempts economic operators from liability when they prove that the damage could not have existed before putting the object into circulation or into service does not apply "[…] *where the defectiveness of the product is due to any of the following, provided that it is within the manufacturer's control:(a) a related service; (b) software, including software updates or upgrades; or (c) the lack of software updates or upgrades necessary to maintain safety*"[1436]. This is indeed an important sign that digital content and services need to be considered as even more relevant in terms of liability consequences (the new PLDU will continue to also apply to traditional objects). No specifications are given on the correct interpretation of the word control, and this will most likely be a new interpretative task for national and CJEU judges.

The third chapter of the PLDU concerns general provisions on liability. It sets rules about the liability of multiple operators, the reduction of liability, the exclusion or limitation of liability and limitation periods[1437]. Article 11 PLDU clarifies that if two economic operators are considered liable for the same damage, they can be held liable jointly or severally, a provision that has remained as it was in the PLD[1438]. Article 12 PLDU instead makes it impossible for MS to reduce liability if the damage was caused by the defectiveness of the product due to a third-party act or omission. Moreover, MS can limit compensation when the damage is also caused by the fault of the victim. Both these rules are the same as Article 10 PLD.

[1432] Article 10 of the ELI PLD draft includes included the risk development exception, the mandatory legal requirements and the non-existence of the defect at the time of making the product available.
[1433] See Article 10(1) (a) (b)PLDU with Article 7 (a); Article 10(1) (c) (PLDU) with 7 (b) PLD; Article 10(1)(d) PLDU with Article 7(d); Article 10(1)(e) PLDU with Article 7(e) PLD, Article 10(1)(f) PLDU and Article 7(f). Only the previous Article 7(c) disappeared on that the product was not manufactured for sale.
[1434] See in particular Article 10(1)(g)
[1435] 10(e) PLDU and 7(e) PLD.
[1436] Article 10 PLDU.
[1437] Articles 11, 12, 13, 14 PLDU.
[1438] Article 12 PLDU.

More than Article 13 PLDU which concerns the exclusion or limitation of liability as in Article 12 PLD, it is advisable to analyse Article 14 PLDU, as it is a complex proviso that should ideally help consumers. Article 14 PLDU, concerning the limitation periods, is influenced by Article 17(1) of the ELI PLD draft as far as both provisions increase the time limit in which the claimant can sue the defendant by one year (from 2 to 3 years)[1439]. In relation to Article 14(1) PLDU, the time limitation of three years starts when all the following three cumulative conditions to claim compensation for product liability exist. This means that the claimant must become aware of the damage, the defectiveness and the identity of the economic operator on the rules based on Article 7 PLDU[1440]. As in the current PLD, it will be national laws that will regulate the suspension, interruption or limitation of that period[1441]. Article 14(2) PLD instead establishes a period of 10 years in which economic operators could be held liable, starting from when the product was entered the market or service, or, if refurbished, from the substantial modification of the object, unless proceedings had already started. As an exception, the economic operator's liability is increased to 15 years whenever a personal injury was latent for 10 years. This last provision clearly stems from cases concerning vaccines or medicinal products, whose side effects may require more than 10 years to become apparent.

Finally, the fourth and last chapter of the PLDU is for final provisions. There are some final instructions concerning the review, repeal and entry into force of the PLDU[1442]. However, the most interesting one in terms of research and study of product liability cases in Europe is Article 15 PLDU. MS will be obliged to "[…] *publish, in an easily accessible and electronic format, any final judgment delivered by their national courts in relation to proceedings launched pursuant to this Directive as well as other relevant final judgments on product liability*."[1443] Moreover the Commission *"[…] may set up and maintain a publicly available database containing the judgments referred to in paragraph 1*"[1444]. This would be extremely useful to the Commission in order to evaluate the effectiveness of the PLDU, but also to make cases concerning IoT much easier to find, a methodological problem that I personally encountered during my research. Moreover, it could make the dialogue between courts concerning ways to balancing consumers' and manufacturers' interests as in Article 8 PLDU more widespread and pave the way for an even wider procedural harmonization.

As a brief first comment on the proposal, the first formal impression is that the Commission has decided to keep more or less the same number of articles in the PLDU, giving the impression that some additional 'patches' have been added to the existing PLD 'fabric'[1445]. This is indeed true to some extent, as the main functioning mechanism is the same in Article 4 PLD and 9(1) PLDU. However, even the smaller details that have been altered in the PLDU

[1439] Article 14 PLDU.
[1440] Article 14 (1) (a)(b)(c) PLDU.
[1441] Article 14(1) PLDU and Article 10(2) PLD.
[1442] Articles 16, 17, 18, 19 and 20 PLD.
[1443] Article 15(1) PLDU.
[1444] Article 15(2) PLDU.
[1445] 20 articles for the PLDU and 22 articles the PLD.

'topography' have had more than a formal impact. Notably, in some articles, old provisions have merely been moved from one place to another, such as Article 5 PLD on the solidarity of the defendants which has become Article 11 PLDU. In other cases, old rules were placed in new frameworks such as the rules concerning damage in Article 9 PLD, which became part of Article 2 PLDU[1446] and to which new elements were added (in this case, the relevance of data). For other dispositions, brand new rules were added as in the case of Article 8 PLD on the disclosure of evidence[1447]. In quite a few other cases, there were old rules or concepts mixed with new ones: one can compare Article 7 PLD on liability exemptions and the new Article 10 PLDU, which also contains exceptions to exemptions in its Article 10(2) PLD. In particular, the exception to the exemption is in Article 10 (1)(c) PLDU concerning the presence of the defect prior to the product being put on the market or into service.

The ELI PLD Draft was more structured and highlighted the connecting points with product safety regulation more precisely. It also introduced post-market surveillance duties and also aimed to harmonise extra-contractual rules[1448]. However, unlike in the suggestion at the end of Chapter V and the ELI PLD draft, the proposed PLDU does not mention personal data damages, pure economic loss damage and market surveillance law. The PLDU has also eliminated any references to nuclear damages (which were excluded from the PLD field of application in Article 14) and it is disappointing that there is no clear reference to sustainability or the environment in the operative text as not even refurbished products are called by their proper name. Only in the explanatory memorandum and in the recital part are there mentions to sustainability and circular economy[1449].

The PLDU has a more general and almost implicit way of framing its connection with cybersecurity and product safety regulations, and never mentions the relevant legislative framework. It only mentions cybersecurity duties and safety requirements (which can be both at national and EU level) and no regulations or directives in particular[1450]. This makes the proposal more readable, and is more likely to stand the test of time, as cybersecurity and safety requirements may change more frequently than this future directive. Leaving the wording so general also has another advantage: private standards, if incorporated in EU or national law, could also cause the defectiveness of a product.

But what about the two main issues that emerged from the analysis of the PLD case law in Section II of Chapter V? To be clearer, does the PLDU answer the issues concerning the identity of the producer and the relationship of the PLDU with the special liability systems in other countries? At first sight, Article 7

[1446] More precisely Article 2(6) PLDU.
[1447] As in the case of Article 8 PLDU on the disclosure of evidence.
[1448] See Article 1 of the ELI PLD Draft.
[1449] In particular, the wording "circular economy" is cited in Recitals 3 and 29; "Environment" is mentioned 5 times in the Explanatory memorandum and the adjective sustainable twice, four times in the memorandum and in Recital 29 PLDU.
[1450] Such as in 6(1)(f) (g) PLDU.

PLDU seems to explain what the allocation of liability will be in detail, so that consumers can always find a subject to ask for compensation. It will be interesting to understand how the CJEU will implement this new "scheme" for allocating liability among the different "economic operators", when with *Fennia v. Philips* it established that the consumer has the right to ask for compensation from whoever presents themselves as producer (manufacturer in the future PLD).

Regarding the coexistence of the PLD with other systems, Article 13 PLD was the origin of many of the cases analysed in Chapter V (often in combination with issues connected to the identity of the producer in Article 3 PLD). Now, as suggested at the end of Chapter V, Article 3 PDLU clarifies that the PLD is a maximum harmonization measure "*unless otherwise provided for by the directive*"[1451]. The detail is that there are no provisions in the whole directive that could actually give the MS an alternative between the different ways to implement the PLDU provisions. Hence, according to the case law commented in Chapter V, the new PLDU will be the main product liability system in the EU and it will apply also to low-risk technological objects such as the IoT ones for the home. This should still leave the special systems based on contractual and fault-based liability that are applied in product liability cases (such as in the *Novo Nordisk Pharma* case) unprejudiced. However, it is uncertain what will become of the CJEU jurisprudence in Article 13 PLD if we think that there were two other elements to consider in the evaluation of a national product liability system compatibility with the PLD. These last two elements were the pre-existence of the national special system to the PLD and the fact that it could be a mechanism used to acquire rights before the entry into force of the PLD. Article 17 PLDU on the repeal and transitional provisions partly answers the previous questions. Article 17(1) PLDU states that PLDU will replace the PLD one year after its entry into force but "[…] *it shall continue to apply with regard to products placed on the market or put into service before that date*". There will therefore be a transition scheme, as in the PLD. Moreover, Article 17(2) PLDU states that any reference to the PLD must be intended, for the future, to be addressed to the PLDU (after its approval) and references between the provisions contained in the two directives will be made in an Annex to the PLDU which has not yet been published. For now, I would say that a more protective approach towards consumers should be adopted, given that AG Szpunar in *Novo Nordisk Pharma* also highlighted that Article 13 PLD's main point regarded previously acquired rights. Hence, in my opinion, the previous CJEU interpretation of Article 13 PLDU will still apply. To sum up, liability systems that are special, existed prior to the PLD (and also the PLDU according to Article 17(1) PLDU), that allowed people to acquire rights and that are fault- or contract-based should continue to exist. One might argue, however, that with the entry into force of the AILP, which partly harmonises fault-based national systems with reference to high-risk algorithms, the number of national product liability systems that differ from the PLD is set to decrease.

[1451] Article 3 PLDU.

In a way, the choice not to render all these maximum harmonization efforts pointless also leads to finally cancelling the monetary threshold to property damage and to extend the application of product liability rationale to connected objects. Moreover, because of Article 17(2) PLDU on the equivalence of the references between the PLD and PLDU, it will finally be possible to connect the PLDU to the new directive on representative actions[1452], which, in Annex 1 (1) mentions the PLD as one of the EU legal acts to which it is applicable[1453]. This means that the PLDU may be challenged much more than its predecessor, the PLD, and it is because of this that the Commission is authorised to set up a common database wherein MS share their cases involving the application of the new PLD. This database would prove useful for several subjects. Firstly, the Commission can use the database to amend the directive according to the rules set out in Article 16 PLDU and test whether there is the need of other harmonising mechanisms. Secondly, national judges could learn of strategies used by colleagues from other countries and use them. Hence it would be easier to trace the diffusion of certain legal models. Thirdly, it would be important for scholars to analyse what the main problems are between theory and practice and to offer solutions. Last but not least, the CJEU will be able to understand the national judges' opinion on the way the new regime of interconnected objects, such as domestic IoT (future IoE) -powered ones, functions.

When referring specifically to the home IoT objects (the future IoE domestic objects) and what these two legislative proposals will change for them the relevance of the PLDU is comparatively much higher than the relevance of the AILP. In fact, the interconnected objects we use in our homes generally are considered low-risk, or, by using the terms of the AI act, low-risk AI systems, hence the AILP does not apply. The PLDU maintains the same rationale as a strict liability mechanism in which it is the consumer's duty to demonstrate the object's defectiveness, the damage it caused and the causal link between the previous two elements. In order to do that it will be helped mainly by the substantive innovation that data and software are products according to the PLDU and by relying on the procedural principles of Articles 8 and 9 PLDU, which concern the disclosure of evidence and the burden of proof. More specifically, Article 9 PLDU lists rebuttable presumptions concerning the elements of defectiveness and the causal link. Furthermore, consumers will have one year more than they do have now to sue the concerned economic operator: Article 14(1) PLDU increases this time-limit from 2 to 3 years. Moreover, the concerned economic operator liability will be increased from 10 to 15 years whenever a personal injury has been latent for ten years according to Article 14 PLDU. Because of its legal basis which is yet again the harmonization clause of Article 114 TFEU, consumer instances are in theory balanced out by the concerned economic operator's ones. As a first remark, the producer does not exist anymore, as it is substituted by the manufacturer which in theory is the first

[1452] Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC.

[1453] The AILP instead has a specific, article 6 AILP, to allow the connection with Directive EU/2020/1828 on representative actions.

subject the consumer should address in case a damage takes place. However, Article 7 PLDU establishes a long list of potentially liable stakeholders that includes importers, authorised market representatives, fulfilment service providers, distributors, refurbished products sellers and online platforms. Each of them could be liable if, starting from the manufacturer, the previous economic operator in the order is either non-EU based or unknown. Initially, this list's original rationale was to update the PLD to the contemporary production and value chains for IoT objects in particular, and for the sharing economy in general[1454]. Nevertheless, doubts might remain as to whether the stakeholders' order chosen by Article 7 PLDU truly reflects the contemporary dynamics of the sharing economy. In fact, most of the IoT manufacturers are based outside the EU[1455]. According to Article 7(5) PLDU, if no previous economic operator is EU-based or known to the consumer, it will be the EU distributors' responsibility to indicate, within one month from the request, the manufacturer's or some other concerned economic operator's identity or contacts. Otherwise, distributors will be held liable. It is true that distributors must bear some risks for importing non-EU goods, but this system risks to exempt non-EU-based manufacturers from liability when one of the reasons for updating the PLD was to increase the safety of connected IoT products for consumers and make the supply and value chain fairer to all the stakeholders involved. The scenario that I have just described does not fully address this kind of needs. It does, however, address the necessity explained in the memorandum of the PLDU that the consumer must not be left without any stakeholder to hold accountable in the EU[1456]. Furthermore, also online platforms, which are accessible through various domestic IoT objects, are at the end of Article 7 PLDU list. In order for a consumer to ask them for compensation, firstly the consumer must exclude all the previous economic operators and make sure that Article 6(3) DSA applies, when, in reality, the online platform is the first point of contact with the product which could later turn out to be defective. If one must draw a balance about whether the new PLDU is truly a harmonization measure, the answer would be that it is, theoretically, slightly more consumer protective than Article 114 TFEU would allow it to be. One could ask whether Article 169 TFEU on consumer protection would have been a more honest legal basis. Moreover, it is not clear how the PLDU will be able to increase the number and activity of EU IoT-based start-ups and companies[1457] if the EU-based ones will be subject to such an extensive implicit duty to manufacture cyber-secure products by taking into consideration product-specific safety requirements, the competent authorities' interventions on these subjects but also the end-users' general expectations concerning the IoT product [1458]. I am not stating that the goal of having safe and cyber-secure IoT products (even domestic ones) is not right. Quite the contrary. What I wonder is whether small-medium EU entrepreneurial realities will have the resources to invest in compliance and research at a sufficient level to compete with international industries which

[1454] Explanatory memorandum PLDU, 7-8.
[1455] Brian Cherok, "The 10 Largest Internet of Things (IoT) Companies In The World, And What They Do", *HC,* December 22, 2022, https://history-computer.com/largest-internet-of-things-iot-companies-in-the-world/.
[1456] Explanatory memorandum PLDU, 7-8.
[1457] Explanatory memorandum PLDU, 7-8.
[1458] See Article 6(1)(f),(g),(h) PLDU.

manufacture and market domestic IoT products on a larger scale and that have more resources to invest in research and compliance.

As a final remark, I would say that the issue of private law liability for IoE objects in the home has received a legislative response that was deeply influenced by legal experts' opinions (even when some of their positions were refused) and by EU business and insurance stakeholders. For the moment, the main problems concerning Article 3 PLD on the producers' (now economic operators') identity and the relationship with other national liability systems of Article 13 PLD have been more or less formally addressed. Litigation and future judgments will provide a more nuanced and precise evaluation of these legal solutions once they are formally adopted.

Bibliography

1. Articles, books, policy briefs and other documents

Abbott, Ryan. “The Reasonable Computer.” *George Washington Law Review* 86,1 (2018):1-45.

Abraham, Kenneth S., and Robert L. Rabin. “Automated Vehicles and Manufacturer Responsibility for Accidents: A New Legal Regime for a New Era.” *Virginia Law Review* 105,1(2019): 129-161.

Abwod, Gregory D., and Elizabeth D. Mynatt. “Charting Past, Present, and Future Research in Ubiquitous Computing.” *ACM Transactions on Computer-Human Interaction*, 7,1 (2000): 29-58.

AI Alliance. Accessed 31 January 2023. https://ec.europa.eu/futurium/en/european-ai-alliance/ai-hleg-steering-group-european-ai-alliance.html.

A-Hed. “VR to the ER: metaverse Early Adopters Prove Accident-Prone.” *The Wall Street Journal*. February 2, 2022. Accessed 31 January 2023. https://www.wsj.com/articles/metaverse-virtual-reality-vr-accident-prone-meta-11643730489.

AI HLEG. “Ethics Guidelines for Trustworthy AI.” 2019. Accessed 31 January 2023 https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

Alberti, Stefano. “L’altra faccia dell’ISP liability. La responsabilità contrattuale del cloud provider fra legge, usi e condizioni negoziali.” *Giustizia Civile* (2014): 1-16.

Albreem Mahmoud A., Abdul Manan Sheikh, Mohammed H. Alsharif, Muzammil Jusoh, and Mohd Nijb Mohd Yasin. “Green Internet of Things (GIoT): Applications, Practices, Awareness, and Challenges.” *IEEE Access* 9(2021): 38833-38858. Accessed 31 January 2023. https://dx.doi.org/10.1109/ACCESS.2021.3061697.

Alemanno, Alberto. “Science & EU Risk Regulation: The Role of Experts in Decision-Making and Judicial Review. EUROPEAN RISK GOVERANANCE - ITS SCIENCE, ITS INCLUSIVENESS AND ITS EFFECTIVENESS, Connex Report Series No. 6, E. Vos, ed., February 2008”. *SSRN* (2014). Accessed 31 January 2023, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1007401.

Ali, Bako, and Awad Ali Ismail. “Cyber and Physical Security Vulnerability Assessment for IoT-based smart homes.” *Sensors* 18,3 (2018):81.7 https://dx.doi.org/10.3390/s18030817.

Alpa, Guido. “Quale modello normativo europeo per l’intelligenza artificiale?.” In *LA RESPONSABILITÀ CIVILE NELL’ERA DIGITALE (Atti della Summer school 2021)*, Valentina V. Cuocci, Francesco Paolo Lops, Cinzia Motti, 3-28. Bari: Cacucci editore, 2022.

Amato, Cristina. “Product Liability and Product Security: Present and Future.” In *Liability for Artificial Intelligence and the Internet of Things Münster Colloquia on EU Law and the Digital Economy IV*, Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer,77-95. Baden-Baden: Beck Nomos,2020.

Ames, James Barr. “The History of Assumpsit.” *Harvard Law Review* 2, 1 (1888):1-19.

Ammar, Reyes, and Samer Salam. *Internet of Things From Hype to Reality The Road to Digitization*. Springer Nature Switzerland, 2019, 2nd ed. https://link.springer.com/book/10.1007/978-3-319-99516-8.

Archdaily. “How to design smart homes. 8 Tips for incorporating domotics into architecture,” *Archdaily*. Accessed 31 January 2023. https://www.archdaily.com/908468/how-to-design-smart-homes-8-tips-for-incorporating-domotics-into-architecture.

Aresta, Marco, and Nikos A. Salingros. “The Importance of Domestic Space in Times of COVID-19.” *Challenges* 12,2 (2021):28. https://dx.doi.org/10.3390/challe12020027.

"Artificial Intelligence (AI) Coined at Dartmouth," *Dartmouth* (official website). Accessed 31 January 2023. https://250.dartmouth.edu/highlights/artificial-intelligence-ai-coined-dartmouth .

Arena, Amedeo. "The Twin Doctrines of Primacy and Pre-emption." in, *Oxford Principles Of European Union Law: The European Union Legal Order: Volume I,* Robert Schütze and Takis Tridimas, 322-349. Oxford: Oxford University Press, 2018. https://dx.doi.org/10.1093/oso/9780199533770.003.0012.

Arnull, Anthony. "Remedies Before National Courts." In *Oxford Principles Of European Union Law: The European Union Legal Order: Volume I*, Robert Schütze and Takis Tridimas, 1011-1039. Oxford: Oxford University Press, 2018. https://dx.doi.org/10.1093/oso/9780199533770.003.0036.

Article 29 Working party. "Opinion 8/2014 on the on Recent Developments on the Internet of Things."2014. Accessed 31 January 2023. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm .

Opinion 1/2010 on the concepts of "controller" and "processor." 2010.

Accessed 31 January 2023 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf. *Opinion 5/2009 on online social networking*, 2009.

Accessed 31 January 2023. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf.

Ashton, Kevin. "That 'Internet of Things' Thing". *RIFID Journal*, 2010.

Attinasi, Maria Grazia., Roberta De Stefani, Erik Frohm, Vanessa Gunnella, Gerrit Koester, Alexandros Melemenidis, and Máté Tóth. "The semiconductor shortage and its implications for euro area trade, productions and prices". *ECB Economic Bulletin Issue 4/2021*. Accessed 31 January 2023. https://www.ecb.europa.eu/pub/economic-bulletin/focus/2021/html/ecb.ebbox202104_06~780de2a8fb.en.html

Ayeba Alfa, Abraham, John Kolo Alhassan, Olayemu Mikail Olaniyi, and Morufu Olalere. "Blockchain technology in IoT systems: current trends, methodology, problems, applications, and future directions," *Journal of Reliable Intelligent Environments* 7(2020): 115-143. https://dx.doi.org/10.1007/s40860-020-00116-z.

Baldin Anna. "EU: Towards the adoption of the NIS 2 Directive" *One Trust Data Governance*. December 2021. Accessed 31 January 2023. https://www.dataguidance.com/opinion/eu-towards-adoption-nis-2-directive.

Balkin, Jack. "The Path of Robotics Law," *California Law Review* 6 (2015):45-60.

Baloup, Julie, Emre Bayamiıoğlu, Aliki Benmayor, Charlotte Ducuing, Lidia Dutkiewicz, Teodora Lalova, Yuliya Miadzveteskaya, and Bert Peeters. *White Paper on the Data Governance Act*. Leuven: CiTiP Working Paper Series, 2021. https://dx.doi.org/10.2139/ssrn.3872703.

Balta-Ozkan, Nazmiye, Oscar Amerigh,i and Boteler Benjamin, "A comparison of consumer perceptions towards smart homes in the UK, Germany and Italy: reflections for policy and future." *Technology Analysis and Strategic Management* 26,10 (2014): 1176-1195. https://dx.doi.org/10.1080/09537325.2014.975788 .

Balta-Ozakan Nazmiye, Rosemary Davidson, Martha Bicket and Lorraine Whitmarsh. "Social barriers to the adoption of smart homes." *Energy Policy* 63 (2013):367-371, http://dx.doi.org/10.1016/j.enpol.2013.08.043.

Bandyopadhyay, Debasis. and Sen, Jaydip. "Internet of Things: Applications and Challenges in Technology and Standardization," *Wireless Personal Communications* 58,1 (2011): 49-69. http://doi.org10.1007/s11277-011-0288-5.

Barocas, Solon,, and Andrew D. Selbst. "Big Data's Disparate Impact." *California Law Review* 104 (2016): 671-732.

Barret, Olivier and Philippe Brun. "Vente: effets- Garantie contre les vices caches." *Répertoire Dalloz* (2018): §§586-594.

Bartholomew, Jem. “Rising popularity of VR headsets sparks 31% rise in insurance claims.” *The Guardian*, February 12, 2022. Accessed 31 January 2023. https://www.theguardian.com/technology/2022/feb/12/rising-popularity-of-vr-headsets-sparks-31-rise-in-insurance-claims.

Battistini, Niccolò, Matteo Falagiarda, Johannes Gareis, Angelina Hackman, and Moreno Roma for the ECB. “The euro area housing market during the COVID-19 pandemic.” *ECB Economic Bullettin*, 7 (2021). https://www.ecb.europa.eu/pub/economic-bulletin/articles/2021/html/ecb.ebart202107_03~36493e7b67.en.html .

BBC News Tech. “Alexa tells a 10-year-old girl to touch live plug with penny.” December 28, 2021. https://www.bbc.com/news/technology-59810383

Beale, Hugh, Bénédicte Fauvarque - Cosson, Jacobien Rutgers,, and Stefan Vogenauer. *Cases Materials and Texts on Contract Law- Ius Commune Casebooks for the Common Law of Europe 3rd*. Oxford: Oxford Hart Publishing, 2019.

Bernard, Vincent, Gabrielle Gallic, Olivier Léon and Catherine Sourd. “Logements suroccupés, personnes agées isolées: des conditions de confinement diverses selon les territoires.” *INSEE FOCUS* 189, Avril 21, 2020. Accessed 31 January 2023. https://www.insee.fr/fr/statistiques/4478728 .

Bertolini, Andrea for the EPRS. *Artificial Intelligence and Civil Liability- Legal Affairs Report*. Brussels: European Parliament, 2020, hereinafter Bertolini.

Bertolini Andrea, and Episcopo Francesca. “The Expert Group’s Report on Liability for Artificial Intelligence and Other Emerging Technologies: A crictical assessment.” *European Journal of Risk Regulation* 12,3 (2021): 644-659 https://dx.doi.org/10.1017/err.2021.30.

Bertuzzi, Luca. “Data governance: new EU law for data-sharing adopted.” *Euractiv*, December 01Castr, 2021. https://www.euractiv.com/section/digital/news/data-governance-new-eu-law-for-data-sharing-adopted/.

Birnbaum, Sheila L. “Unmasking the Test for Design Defect: From Negligence [to Warranty] to Strict Liability to Negligence.” *Vanderbilt Law Review* 33, 3(1980): 593-649.

Blandiford, Ann, Janet Wesson, René Amalberti, Raed Alhazme and Ragad Allwihan. “Opportunities and challenges for telehealth within, and beyond, a pandemic.” *The Lancet Global Health* 8,11(2020). https://dx.doi.org/10.1016/S2214-109X(20)30362-4.

Borges, Georg. “New Liability Concepts: the Potential of Insurance and Compensation Funds.” In *Liability for Artificial Intelligence and the Internet of Things. Münster Colloquia on EU Law and the Digital Economy*, Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer,145-163. Baden Baden: Nomos Verlag- Hart Publishing, 2020.

Borghetti, Jean-Sébastien. “Product Liability in France.” In *European Product Liability: An Analysis of the State of the Art in the Era of New Technologies*, Piotr Machnikowski 205-236. Cambridge, Portland Antwerp: Intersentia, 2016.

Borghetti, Jean-Sebastien, Marta dos Santos Silva, Duncan Fairgrieve, Pedro García, Anne Keirse, Piotr Machnikowski, Eleonora Rajneri, Christoph Schmon, Vibe Ulbeck, Vera Vallone and, Herbert Zech. “Relevance of Risk-benefit for Assessing Defectiveness of a Product: A Comparative Study of Thirteen European Legal Systems.” *European Review of Private Law* 29,1 (2021): 91-132.

Bottero, Marta, Marina Bravi, Caterina Caprioli, Federico Dell’Anna, Marta Dell’Ovo, and Alessandra Oppio. “New Housing Preferences in the COVID-19 Era: A Best-to-Worst Scaling Experiment.” In *Computational Science and its Applications- ICCSA 2021* Osvaldo Gervasi et al., 120-129. LNCS, 2021.

Boyne Shawn Marie. “Data Protection in the United States,” *American Journal of Comparative Law* 66,8 (2018) 28, https://dx.doi.org//10.1093/ajcl/avy016.

Breton, Thierry. “Sneak-peek how the Commission will enforce the DMA and DSA.”, Linkedin Post. July 6, 2022. Accessed 31 January 2023.https://www.linkedin.com/pulse/sneak-peek-how-commission-enforce-

dsa-dma-thierry-breton https://www.consilium.europa.eu/en/press/press-releases/2022/04/23/digital-services-act-council-and-european-parliament-reach-deal-on-a-safer-online-space/ .

Busch, Christoph. "Does the Amazon Dash Button Violate EU Consumer Law? Balancing Consumer Protection and Technological Innovation in the Internet of Things." *Journal of European Consumer and Market Law* 2(2018): 78-80. "The Future of pre-contractual information duties." In *Research Handbook on EU Consumer and Contract Law*, Christian Twigg-Flesner, 221-240. Cheltenham, UK, Northampton, USA: Edward Elgar publishing, 2016.

Busch, Christoph, and Vanessa, Mak. "Putting the Digital Services Act into Context: Bridging the Gap between EU Consumer Law and Platform Regulation." *Journal of European Consumer and Market Law* 3(2021): 109-115.

Bussani, Mauro. "LE FUNZIONI DELLE FUNZIONI DELLA RESPONSABILITÀ CIVILE," *Rivista di diritto civile* 2 (2022): 264-306; *L'Illecito Civile*. Napoli: Edizioni Scientifiche Italiane, 2020.

Bussani, Mauro and Marta Infantino. "The Many Cultures of Tort Liability." In *Comparative Tort Law. Global Perspectives*, Mauro Bussani, Anthony J. Sebok, 9-34. Cheltenham: Edward Elgar, 2021.

Caffarra, Cristina and Fiona Scott Morton. "The European Commission Digital Markets Act: A translation." *VOXEu CEPR*. Accessed 31 January 2023. https://voxeu.org/article/european-commission-digital-markets-act-translation.

Calabresi, Guido, and Al Mureden, Enrico. *Driverless cars*. Bologna: Il Mulino, 2021.

Calabresi, Guido and A. Douglas Melamed. "Property Rules, Liability Rules, and Inalienability: One View of the Cathedral." *Harvard Law Review* 85,6 (1972): 1089-1128.

Calo, Ryan. "Robotics and the Lessons of Cyberlaw." *California Law Review* 103, 3(2015):515-564.

Cannarsa, Michel. *LA RESPONSABILITÉ DU FAIT DES PRODUITS DÉFECTUEUX. ÉTUDE COMPARATIVE.* Milano: Giuffrè editore, 2005.

Carlson, Colin J., Gregory F. Albery, Cory Merow, Christopher H. Trisos, Casey M. Zipfel, Evan A.Eskew, Kevin J. Olival, Noam Ross, and Shweta Bansal. "Climate change increases cross-species viral transmission risk." *Nature* 607(2022): 555-561. https://dx.doi.org/10.1038/s41586-022-04788-w.

Castronovo, Vincenzo. *La responsabilità civile*. Milano: Giuffrè, 2018.

Chagal-Feferkorn, Karni "AM I AN ALGORITHM OR A PRODUCT? WHEN PRODUCTS LIABILITY SHOULD APPLY TO ALGORITHMIC DECISION-MAKERS." *Stanford Law & Policy Review* 30 (2019):61-114.

Chen, Jiahong, Lilian Edwards, Lachlan Urquart, and Derek McAuley. "Who Is Responsible for Data Processing in Smart Homes? Reconsidering Joint Controllership and the Household Exemption." *International Data Privacy Law* 10,4(2020): 279-293, https://academic.oup.com/idpl/article/10/4/279/5900395.

Cherok, Brian. "The 10 Largest Internet of Things (IoT) Companies In The World, And What They Do." *HC*, 22 December 2022. https://history-computer.com/largest-internet-of-things-iot-companies-in-the-world/.

Chevuru, Sunil, Anil Kumar, Ned Smith, and David M. Wheeler. *Demystifing Internet of Things Security. Successful IoT Device/Edge and Platform Security Deployment*. New York: Springer Apress Open, 2020.

Chirico, Filomena. "Digital Markets Act: A Regulatory Perspective." *Journal of European Competition Law and Practice* 12,7 (2021): 493-499.

Choi, Bryan H. "Crashworthy Code." *Washington Law Review* 94(2019): 39-117.

Chui Michael, Mark Collins ,and Mark Patel. "IoT Value set to accelerate through 2030: Where and how to capture it?," *McKinsey Digital*, 9 November 2021, https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/iot-value-set-to-accelerate-through-2030-where-and-how-to-capture-it.

Chun, Yung, and Michal Grinstein-Weiss. "Housing inequality gets worse as the COVID-19 pandemic is prolonged." *Brookings Edu*. December 18, 2020. Accessed 31 January 2023.

https://www.brookings.edu/blog/up-front/2020/12/18/housing-inequality-gets-worse-as-the-covid-19-pandemic-is-prolonged/.

CISCO, *Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are. White Paper* (2015):1-6. Accessed 31 January 2023. https://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/computing-overview.pdf.

Clarke, Áine. "Adapting liability rules to the digital age and artificial intelligence." *Insurance Europe*. 16 February 2021. Accessed 31 January 2023. https://www.insuranceeurope.eu/mediaitem/46c3d081-6db4-4d62-af388b356591f3dc/Adapting%20liability%20rules%20to%20the%20digital%20age%20and%20artificial%20intelligence.pdf.

Clifford Law Offices. "The Dangers of Driverless Cars." *National Law Review* 12,116 (2021). 5 May 2021. Accessed 31 January 2023, https://www.natlawreview.com/article/dangers-driverless-cars

CNIL. *À votre écoute. Exploration des enjeux éthiques, techniques et juridiques des assistants vocaux*. CNIL: Paris, 2020.

Costa, Luiz. "Data Protection Law, Processes and Freedoms." In *Virtuality and Capabilities in a World of Ambient Intelligence*, Luiz Costa:137-170. Switzerland: Springer International, 2016.

Council of the European Union. "Confidentiality of electronic communications: Council agrees its position on ePrivacy rules." European Council, Council of the European Union. Accessed 31 January 2023, https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf.

Council of the European Union, "Digital Services Act: Council and European Parliament provisional agreement for making the internet a Safer Place." June 15, 2022. Accessed 31 January 2023, https://www.consilium.europa.eu/en/press/press-releases/2022/04/23/digital-services-act-council-and-european-parliament-reach-deal-on-a-safer-online-space/ .

CNIL. "Cookies: the CNIL fines GOOGLE a total of 150 million euros and Facebook 60 million euros for non-compliance with French legislation." *CNIL*. Accessed 31 January 2023. https://www.cnil.fr/en/cookies-cnil-fines-google-total-150-million-euros-and-facebook-60-million-euros-non-compliance .

Com-Art, "Maison connectée: les innovations majeurs de 2020 en termes de domotique," Accessed 31 January 2023, https://www.comart-design.com/maison-connectee-les-innovations-majeures-de-2020-en-termes-de-domotique/.

Colombi Ciacchi, Aurelia, Christopher Hodges, Barend van Leeuwen, Vanessa Mak, Hans Micklitz, Isabelle Rueda, Esther van Schagen, and Stephen Weatherhill. "Position Paper on the Fitness Check of EU Consumer Law." *European Review of Private Law* 26,5(2018): 703-706.

Comandè, Giovanni. "Multilayered (Accountable) Liability for Artificial Intelligence." In *Liability for Artificial Intelligence and the Internet of Things. Münster Colloquia on EU Law and the Digital Economy,* Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer, 165-183. Baden Baden: Nomos Verlag- Hart Publishing, 2019; "Product Liability in Italy." In *European Product Liability: An Analysis of the State of the Art in the Era of New Technologies*, Piotr Machnikowski, 276-309. Cambridge, Portland Antwerp: Intersentia, 2016

Contreras, Jorges. "Origins of FRAND Licensing Commitments in the United States and Europe," in *The Cambridge Handbook of Technical and Standardization Law. Competition, Antitrust, and Patents*, Jorge Contreras, 149-169. Cambridge: Cambridge University Press, 2017. https://dx.doi.org/10.1017/9781316416723.012.

Craig, Paul, and Gráinne De Burca. *EU Law. Texts, Cases and Materials (5th edition)*. Oxford: Oxford University Press, 2015.

Crémer, Jacques, Yves-Alexandre De Montjoye, and Heike Schweitzer. *Competition policy for the digital era*. Luxembourg: European Commission, 2019. https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf.

Crootof, Rebecca. "The Internet of Torts: Expanding civil liability standards to address corporate remote interference." *Duke Law Journal* 69,3 (2019): 583-667.

Custers, Bart. “New digital rights: Imagining additional fundamental rights for the digital era.” *Computer Law and Security Review* 44(2022):10536. https://dx.doi.org/10.1016/j.clsr.2021.105636.

Cygan, Adam. “A step too far? Constitutional objections to harmonization of EU consumer and Contract Law.” In *Research Handbook on EU Consumer and Contract Law*, Christian Twigg-Flesner, 13-34. .Cheltenham, UK, Northampton, USA: Edward Elgar publishing, 2016.

Darby, Sarah J. “Smart technology in the home: time for more clarity.” *Building Research and Information* 46,1 (2018): 140-147. https://dx.doi.org/10.1080/09613218.2017.1301707.

Davies, Bill. “*Internationale Handelsgesellschaft* and the Miscalculation at the Inception of the ECH’s Human Rights Jurisprudence.” In *EU Law Stories. Contextual and Critical Histories of European Jurisprudence*, Fernanda Nicola and Bill Davis, 157-177. Cambridge: Cambridge University Press, 2017. https://dx.doi.org/10.1017/9781316340479.009.

Davis, Fred D. “Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Technology,” *MIS Quarterly* 13,3 (1989):319-340

Davis, Nicholas, Mark Esposito, and Landry Signé. “The anatomy of technological regulation.” *Brookings*, February 17, 2022. https://www.brookings.edu/opinions/the-anatomy-of-technology-regulation/ .

De Conca, Silvia. “Between a rock and a hard place: owners of smart speakers and joint control.” *SCRIPT-ed* 17,2 (2020): 238-268. https://dx.doi.org/10.2966/scrip.170220.238.

De Franceschi, Alberto. *La Vendita dei Beni con Elementi Digitali.* Napoli: Edizioni Scientifiche Italiane, 2019.

De Gregorio, Giovanni. “Digital Constitutionalism: An Introduction.” In *Digital Constitutionalism in Europe*, Giovanni De Gregorio, 1-37. Cambridge: Cambridge University Press, 2022. https://dx.doi.org/10.1017/9781009071215.002. “The Law of Platforms,” In *Digital Constitutionalism in Europe*, Giovanni De Gregorio, 80-122. Cambridge: Cambridge University Press, 2022. https://dx.doi.org/10.1017/9781009071215.004.

De Meeus, Charlotte. “The Product Liability Directive at the Age of the Digital Industrial Revolution: Fit for Innovation?.” *Journal of European Consumer and Market Law* 29,4 (2019):149-154.

Dengler, Sebastian, Abdalkarim Awad, and Falko Dressler. “Sensor Actuator Network in Smart Homes for Supporting Elderly and Handicapped people”. In 21st International Conference on Advanced Information Networking and Applications (AINA 2007), Workshops Proceedings, Volume 2, May 21-23, 2007, Niagara Falls, Canada, *IEEE*. https://dx.doi.org/10.1109/AINAW.2007.325 .

Deoras, Shristi. “First Ever IoT Device – The Internet Toaster”. *Analytics India Magazine*. August 5, 2016.

https://analyticsindiamag.com/first-ever-iot-device-the-internet-toaster/.

Determann, Lothar and Perens, Bruce. “Open Cars.” *Berkley Technology Law Journal* 32,2(2017): 915-988.

Ding, Dan. Rory A. Cooper, Paul F. Pasquina and Lavinia Fici-Pasquina. “Sensor technology for smart homes.” *Maturitas* 69,2 (2011):131-136. https://dx.doi.org/10.1016/j.maturitas.2011.03.016.

Dinh, Hoang T., Chonho Lee, Dusit Niyato, and Ping Wang. “A survey of mobile cloud computing: architecture, applications, and approaches.” *Wireless Communications and Mobile Computing* 13 (2013):1597-1611. https://dx.doi.org/10.1002/wcm.1203.

Drexl, Josef. “Designing Competitive Markets for Industrial Data - Between Propertisation and Access.” JIPITEC 4 (2017) 257- 292

Ducato, Rossana. “LA LESIONE DELLA PRIVACY DI FRONTE ALLA "SOGLIA DI RISARCIBILITÀ": LA NUOVA MAGINOT DEL DANNO NON PATRIMONIALE?.” *Trento Law and Technology Research Group.* (2016): 125-148.

Ducuing, Charlotte. “Understanding the rule of prevalence in the NIS directive: C-ITS as a case study” *Computer Law and Security Review* 40 (2021):105514. https://dx.doi.org/10.1016/j.clsr.2020.105514.

Ebers, Martin. “Standardizing AI. The Case of the European Commission’s Proposal for an ‘Artificial Intelligence Act’.” In *The Cambridge Handbook of Artificial Intelligence. Global Perspectives on Law and Ethics*, Larry A. Dimatteo, Cristina Poncibò and Michel Cannarsa, 321-344. Cambridge: Cambridge University Press, 2022; “Standardizing Artificial Intelligence. A Critical Assessment of the European Commission’s Proposal for an Artificial Intelligence Act.” *Robotics & AI Law Society (RAILS) blog*. Accessed 31 January 2023. https://blog.ai-laws.org/standardizing-artificial-intelligence/.

EDPB. *Guidelines 07/2020 on the concepts of controller and processor in the GDPR - Version 2.0.* 2021. Accessed 31 January 2023. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en.

EDPB-EDPS. *Joint Opinion 2 / 2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)* Adopted on 4 May 2022. Accessed 31 January 2023. https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-22022-proposal-european_en .

Edwards Keith W., and Rebecca E. Grinter. “At Home with Ubiquitous Computing: Seven Challenges.” In *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, Gregory D. Abwod, Barry Burmitt and Steven Shafer, 201: 256. Berlin-Heidelberg :Springer Verlag, 2001. https://dx.doi.org/10.1007/3-540-45427-6_22.

Efroni, Zohar., Jakob Metzger, Mischau Lena and Marie Schrimbeck. “Privacy icons: A risk-based approach to visualisation of data processing.” *European Data Protection Law Review* 5,3 (2019): 352-366. https://dx.doi.org/10.21552/edpl/2019/3/9

Efstathiou, Konstantinos. “Breaking up big companies and market power concerntration.” *Bruegel*, April 29, 2019. Accessed 31 January 2023. https://www.bruegel.org/blog-post/breaking-big-companies-and-market-power-concentration.

ELI Draft of a Revised Product Liability Directive,” ELI Website, Accessed 31 January 2023, https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Draft_of_a_Revised_Product_Liability_Directive.pdf.

Elvy, Stacy-Ann. “Privacy in the Internet of Things World.” In *A Commercial Law of Privacy and security for the Internet of Things*, Stacy-Ann Elvy, 25-58. Cambridge: Cambridge University Press, 2021; “The Current privacy and Data Security Legal Landscape,” in *A Commercial Law of Privacy and security for the Internet of Things*, Stacy-Ann Elvy,80-116, Cambridge: Cambridge University Press, 2021.

Encyclopædia Britannica. “Assumpsit”. 1911, v.2. Accessed 31 January 2023.

https://en.wikisource.org/wiki/1911_Encyclop%C3%A6dia_Britannica/Assumpsit.

Engler, Alex. “The EU and U.S. are starting to align on AI regulation.” *Brookings*, February 1, 2022. https://www.brookings.edu/blog/techtank/2022/02/01/the-eu-and-u-s-are-starting-to-align-on-ai-regulation/.

ENISA, *IoT and Smart Infrastructures* (presentation page), Accessed 31 January 2023, https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot .

ENISA. *Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures.* ENISA, 2017.

ENISA, *Threat and Risk Managment- Publications* (presentation page), Accessed 31 January 2023, https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends?tab=publications .

European Commission. “Internet of things. An action plan for Europe.” 2009. Accessed 31 January 2023. http://ec.europa.eu/information_society/policy/rfid/documents/commiot2009.pdf%.

European Commission. “EU-Ecolabel.” Accessed 31 January 2023.https://environment.ec.europa.eu/topics/circular-economy/eu-ecolabel-home_en.

European Commission. “New Legislative Framework.” *European Commission*. Accessed 31 January 2023. https://ec.europa.eu/growth/single-market/goods/new-legislative-framework_es

European Commission. “5G.” Accessed 31 January 2023. https://digital-strategy.ec.europa.eu/en/policies/5g.

European Commission: “Antitrust: Commission launches sector inquiry into the consumer Internet of Things (IoT)”. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1326

European Commission. Internal Market (webpage). “*Rare earth elements, permanent magnets and motors*”. Accessed 31 January 2023. https://ec.europa.eu/growth/sectors/raw-materials/areas-specific-interest/rare-earth-elements-permanent-magnets-and-motors_en

European Commission. “European Chips Act: Communication Regulation Joint Undertaking and Recommendation.” February 8, 2022. Accessed 31 January 2023. https://digital-strategy.ec.europa.eu/en/library/european-chips-act-communication-regulation-joint-undertaking-and-recommendation.

European Commission, “ EU-US Trade and Technology Council: strengthening our renewed partnership in turbulent times,” EU Commission Press release, May 16, 2022, Accessed 31 January 2023, https://ec.europa.eu/info/strategy/priorities-2019-2024/stronger-europe-world/eu-us-trade-and-technology-council_en.

Expert Group on Liability and New Technologies. *Liability for Artificial Intelligence Report from the Expert Group on Liability and New Technologies-New Technologies Formation*. Brussels: European Commission, 2019. Accessed 31 January 2023. https://op.europa.eu/en/publication-detail/-/publication/1c5e30be-1197-11ea-8c1f-01aa75ed71a1/language-en

European Group on Tort Law. *Principles of European Tort Law*. Accessed 31 January 2023., http://www.egtl.org/docs/PETL.pdf.

European Parliament. *Civil Law Rules on Robotics European Parliament resolution (2015/2103(INL))*. Accessed 31 January 2023. http://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.pdf.

European Parliament, “The NIS 2 Directive: A high common level of cybersecuty in the EU.” December 1, 2021. Accessed 31 January 2023. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333

Ezrachi, Ariel and Maurice E. Stucke. “Artificial intelligence & collusion: When computers inhibit competition.” *University of Illinois Law Review* 5 (2017): 1775-1810.

Fagan, Michael., Katerina N. Megas, Karen Scarafone, and Matthew Smith. *NISTIR 8259 A IoT Device Cybersecurity Capability Core Baseline* NIST website. Accessed 31 January 2023. https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259A.pdf.

Fagan, Michael., Katerina N. Megas, Karen Scarafone, and Matthew Smith. *NISTIR 8259 Cybersecurity Activities for IoT Device Manufacturers*, NIST website. 2020. Accessed 31 January 2023. https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259.pdf

Fairgrieve, Duncan, Howells Geraint, Møgelvang-Hansen, Peter, Straetmans, Gert, Verhoeven, Dimitri, Machnikowski, Janssen André “Product Liability Directive,” in *European Product Liability: An Analysis of the State of the Art in the Era of New Technologies*, Piotr Machnikowski, 17-108. Antwerp, Cambridge, Portland: Intersentia, 2016.

Fazio, Antonino. “IL NESSO CAUSALE NELLA RESPONSABILITÀ OGGETTIVA E SEMI OGGETTIVA.” In *Trattati Giuridici Omnia-La Responsabilità Civile, vol III*, Paolo Cendon, 3533-3584. Torino: Utet Giuridica, 2020, 2nd ed.

FDA. ‘A History of Medical Device Regulation & Oversight in the United States.” *FDA* (Official Website). Accessed 31 January 2023. https://www.fda.gov/medical-devices/overview-device-regulation/history-medical-device-regulation-oversight-united-states.

Finck, Michelle. “Cobwebs of control: the two imaginations of the data controller in EU law.” *International Data Privacy Law* 11,4(2021):333-347. https://dx.doi.org/10.1093/idpl/ipab017.

Fletcher, George P. “Fairness and Utility in Tort Theory”. *Harvard Law Review* 85,3 (1972) :537-573.

Floridi, Luciano. *The 4th Revolution*. Oxford: Oxford University Press, 2014.

Frank-Jackson, Demetria D. “THE MEDICAL DEVICE FEDERAL PREEMPTION TRILOGY: SALVAGING DUE PROCESS FOR INJURED PATIENTS.” *Southern Illinois Law Review* 35(2019): 453-497.

Franklin, Marc A. " When Worlds Collide: Liability Theories and Disclaimers in the Defective-Product Cases.” *Stanford Law Review* 18,6 (1966): 974-1020.

Fundamental Rights Agency of the EU and the Council of Europe. *Handbook of European Data Protection Law*. Luxembourg: Fundamental Rights Agency of the EU and the Council of Europe, 2018. https://dx.doi.org/10.2811/343461.

Garante Privacy. “‘Transparent Information’: winners of the contest launched by Italian SA announced”. Accessed 31 January 2023. https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9727383#english.

Garben, Sacha. “Article 169 TFEU.” In *The EU Treaties and the Charter of Fundamental Rights: A Commentary*, Manuel Kellerbauer, Marcus Klamert and Jonathan Tomkin,1456-1466. Oxford University Press: Oxford, 2019. https://dx.doi.org/10.1093/oso/9780198759393.003.280.

García- Corretjer, Marialejandra, Raquel Ros, Roger Mallol, and David Miralles. “Empathy as an engaging strategy in social robotics: a pilot study.” *User Modeling and User-Adapted Interaction* 2022. https://dx.doi.org/10.1007/s11257-022-09322-1.

Gasser, Urs, and John Palfrey. “Fostering innovation and trade in the global information society: The different facets and roles of interoperability” In *Trade Governance in the Digital Age-World Economic Forum*, Mira Burri and Thomas Cottier, 121-151. Cambridge: Cambridge University Press, 2012.

G.C.L. “The implied Warranty of Merchantability. Smith v. Hensley.” *Virginia Law Review* 48, 1(1962): 152-172.

“GDPR Violations in Germany: Civil Damages Actions on the Rise.” *Latham & Watkins Litigation & Trial and Data Privacy & Security Practices*. December 18, 2020. Accessed 31 January 2023. https://www.lw.com/admin/upload/SiteAttachments/Alert%202821v7.pdf

Geigner, Thimothy. “The Epic Crime Spree Unleashed by Onity’s Ambivalence To Its Easily Hacked Hotel Locks,” *techdirt*, September1 , 2017. Accessed 31 January 2023. https://www.techdirt.com/2017/09/01/epic-crime-spree-unleashed-onitys-ambivalence-to-easily-hacked-hotel-locks/.

Geistfield, Mark. “A Roadmap for Autonomous Vehicles: State Tort Liability, Automobile Insurance, and Federal Safety Regulation.” *California Law Review* 105(2017): 1611- 1694.

Gennari, Francesca. “Liability for IoT Standards in the EU. And yet it moves?”. *Robotics & AI Law Society (RAILS) blog*, June 17, 2022. Accessed 31 January 2023. https://blog.ai-laws.org/liability-for-iot-standards-in-the-eu-and-yet-it-moves/; “Standard Setting Organisations for the IoT: How To Ensure a Better Degree of Liability?.” *Masaryk University Journal of Law and Technology* 15,2 (2021): 153-173. https://dx.doi.org/10.5817/MUJLT2021-2-1.

Gestalten. “Henning Larsen: Will the Pandemic Change Architecture?.” February 2021. Accessed 31 January 2023. https://gestalten.com/blogs/journal/henning-larsen-will-the-pandemic-change-architecture.

Giacobbe, Alyssa. “How the COVID-19 Pandemic Will Change the Built Environment.” *AD*. March 18, 2020. Accessed 31 January 2023. https://www.architecturaldigest.com/story/covid-19-design.

Gillis Talia B. “The Input Fallacy.” *Minnesota Law Review*, forthcoming 2022. Accessed 31 January 2023. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3571266.

Gleeson, Niamh, and Ian Walden. “Cloud computing, standards and the law.” In *Cloud Computing Law*, Christopher Millard, 501-524. Oxford: Oxford University Press, 2021, 2nd ed. https://doi.org/10.1093/oso/9780198716662.003.0015.

Gómez-Portes, Cristian, David Vallejo, Ana I. Molina, and Carmen Lacave. “Automatic Generation of Customised Exergames for Home Rehabilitation on physical mobility constraints and key performance indicators.” in *Intelligent Environments*, Carlos Iglesisas et al. (Amsterdam: IOS Press,2020): 29, https://doi.org/10.3233/AISE200020.

Gorman, Leta. “The Era of the Internet of Things: Can Product Liability Laws Keep Up?.” *Defense Counsel Journal* 84,3(2017):1-9.

Graziadei, Michele. “The European Court of Justice at Work: Comparative Law on Stage Behind the Scenes,” *Journal of Civil Law Studies* 13,1 (2020): 5-31. Graziadei, Michele and Riccardo De Caria. “THE « CONSTITUTIONAL TRADITIONS COMMON TO THE MEMBER STATES » IN THE CASE-LAW OF THE EUROPEAN COURT OF JUSTICE: JUDICIAL DIALOGUE AT ITS FINEST- estratto.” *Rivista Trimestrale di Diritto Pubblico* 4 (2017): 949-971. “Fostering a European legal identity through contract and consumer law,” in *Research Handbook on EU Consumer and Contract Law*, Christian Twigg-Flesner, 82-108. Cheltenham, UK, Northampton, USA: Edward Elgar publishing, 2016.

Green, Michael, and Jonathan Cardi. “Product Liability in the United States of America.” In *European Product Liability: An Analysis of the State of the Art in the Era of New Technologies*, Piotr Machnikowski, 576-616. Cambridge, Portland Antwerp: Intersentia, 2016.

Guerra, Giorgia. *La sicurezza degli artefatti robotici in prospettiva comparatistica. Dal cambiamento tecnologico all’adattamento giuridico*. Bologna: Il Mulino, 2018.

Gupta, Sakshi. “Natural Language Processing Use Case- How Do Personal Assistant Apps Work?.” *Springboard*. June 10, 2020. Accessed 31 January 2023. https://www.springboard.com/blog/data-science/nlp-use-cases/.

Hélaine, Cédric. “De la bonne utilisation de la garantie des vices cachés dans une chaîne de contrats.” *Dalloz Actualité*, July, 06 2022.

Herndon, Astead W. “Elizabeth Warren Proposes Breaking Up Tech Giants Like Amazon and Facebook.” *The New York Times* March 8, 2019, https://www.nytimes.com/2019/03/08/us/politics/elizabeth-warren-amazon.html.

Holle, Marie-Louise, and Peter Møgelvang-Hansen. “Product Liability in Denmark.” In *European Product Liability: An Analysis of the State of the Art in the Era of New Technologies,* Piotr Machnikowski, 155-172. Cambridge, Portland Antwerp: Intersentia, 2016.

Home Stratosphere. “Smart Home Sensors.” May 18, 2020. Accessed 31 January 2023. https://www.homestratosphere.com/smart-home-sensors/.

Hoofingale, Chris Jay. “Designing for Consent.” *Journal of European Consumer and Market Law* 4(2018):162-171.

Hornung, Gerrit, and Stefan Bauer, “Privacy Through Certification?: The New Certification Scheme of the General Data Protection Regulation,” In *Certification Trust Accountability*, Peter Rott, 109-142. Cham, Switzerland: Springer Nature, 2019.

Hu, Jun-Ho, and Seo Yeong-Seok. “Understanding Edge Computing: Engineering Evolution with Artificial Intelligence.” *IEEE Access* 7(2019):164229. https://dx.doi.org/10.1109/ACCESS.2019.2945338.

Hubbard, F. Patrick. “‘Sophisticated Robots’: Balancing Liability, Regulation and Innovation.” *University of Florida Law Review* 66(2014): 1811-1872.

ILO and WHO, *Healthy and Safe Telework. Technical Brief.* Geneva, 2021. Accessed 31 January 2023, https://www.who.int/publications/i/item/9789240040977

International Encyclopedia of Cyber Law. "§4. INTERPRETING SOFTWARE CONTRACTS" 5813249 (C.C.H.), 2020 WL 5813249.

IMC Newsdesk. "Digital health investments surge 79 per cent." *Imc, IoT M2m council*, Accessed 31 January 2023. https://www.iotm2mcouncil.org/iot-library/news/connected-health-news/digital-health-investments-surge-79-per-cent/.

"Introduction to Sensors and Transducers." *Electronics Hub. Projects, Tutorials, Reviews and Kits*. February 19, 2019. https://www.electronicshub.org/sensors-and-transducers-introduction/ .

"IoE", Last JD RIoE Website. 2019, Accessed 31 January 2023. https://last-jd-rioe.eu/.

Ishiguro, Kazuo. *Klara and the Sun*. London: Faber&Faber, 2021.

ITU, *Recommendation ITU-T Y 2060 (6/2012) Overview of the Internet of Things*. Geneva, 2012. https://handle.itu.int/11.1002/1000/11559.

Jain, Shruti. "Can blockchain accelerate Internet of Things (IoT) adoption?." Accessed 31 January 2023. https://www2.deloitte.com/ch/en/pages/innovation/articles/blockchain-accelerate-iot-adoption.html

Jansen, Nils, and Reinhard Zimmermann. "General Introduction. European Contract Laws. Foundation Commentaries, Synthesis," in *Commentaries on European Contract Laws* Nils Jansen and Richard Zimmermann, 1-18. Oxford: Oxford University Press, 2018. https://dx.doi.org/10.1093/oso/9780198790693.003.0001. " A EUROPEAN CIVIL CODE IN ALL BUT NAME: DISCUSSING THE NATURE AND PURPOSES OF THE DRAFT COMMON FRAME OF REFERENCE." *Cambridge Law Journal* 69,1 (2010): 98-112. https://dx.doi.org/10.1017/S000819731000019X.

Jarman, Holly, Sarah Rozenblum, and Tiffany J Huang. "Neither protective nor harmonized: The crossborder regulation of medical devices in the EU." *Health Economics, Policy and Law* 16,1(2021):51-63.

Jobin, Anna, Marcello Ienca, and Effy Vayena. "Artificial Intelligence: the global landscape of ethics guidelines," *Nature Machine Intelligence* 1,9 (2019): 389-399.

Kalamees, Piia. "Goods with Digital Elements and the Seller's Updating Obligation." *JIPITEC* 12 (2021):131-142.

Karagul, Banu Inan., Meral Seker and Cansu Aykut. "Investigating students' digital literacy levels during online education due to covid-19 pandemic." *Sustainability* 13,21(2021):11878. https://dx.doi.org/10.3390/su132111878.

Karner, Ernst. "Liability for Robotics: current Rules, Challenges and the Need for Innovative Concepts." In *Liability for Artificial Intelligence and the Internet of Things Münster Colloquia on EU Law and the Digital Economy IV*, Sebastian Lohsse, Reiner Schulze et Dirk Staudenmayer, 117-143. Baden-Baden: Beck Nomos,2020.

Karner, Ernst, Bernard A. Koch and Mark Geistfield. *Comparative Law Study on Civil Liability for Artificial Intelligence*. Luxembourg: European Commission, 2021. https://dx.doi.org/10.2838/77360.

Kanižaj, Igor, and Brites, Maria José. "Digital Literacy of Older People and the Role of Intergenerational Approach in Supporting Their Competencies in Times of Covid-19 Pandemic." In *Human Aspects of IT for the Aged Population. Design, Interaction and Technology Acceptance. HCII 2022. Lecture Notes in Computer Science,* Gao, Q., Zhou, J. (eds) vol 13330, 335-345.

Springer, Cham, 2022. https://dx.doi.org/10.1007/978-3-031-05581-2_25.

Kaye, Elliot F. and Jonathan D. Midgett for CPSC. "A FRAMEWORK OF SAFETY for the Internet of Things: Considerations for Consumer Products Safety." January 31, 2019. Accessed 31 January 2023. https://www.cpsc.gov/s3fs-public/A_Framework_for_Safety_Across_the_Internet_of_Things_1-31-2019.pdf.

Kellerbauer, Manuel. “Article 114.” In *The EU Treaties and the Charter of Fundamental Rights: A Commentary*, Manuel Kellerbauer, Marcus Klamert and Jonathan Tomkin,1235-1255. Oxford: Oxford University Press, 2019. https://dx.doi.org/10.1093/oso/9780198759393.003.280

Klamert, Marcus. “Article 4 TFEU.” In *The EU Treaties and the Charter of Fundamental Rights*, Manuel Kellerbauer, Marcus Klamert and Jonathan Tomkin, 35-60. Oxford: Oxford University Press, 2019.https://dx.doi.org/10.1093/oso/9780198759393.003.7.

Kleinman, Zoe. “The abortion privacy dangers in period trackers and apps.” BBC News. June 28, 2022. https://www.bbc.com/news/technology-61952794 .

Koch, Bernard A., Jean- Sébastien Borghetti, Piotr Machinowski, Pascal Pichonnaz, Teresa Rodríguez de las Heras Ballell, Christian Twigg-Flesner, and Christiane Wendehorst. “Response of the European Law Institute Public Consultation on Civil Liability Adapting liability rules to the digital age and artificial intelligence. ” Accessed 31 January 2023, https://europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Response_to_Public_Consultation_on_Civil_Liability.pdf.

Koch, Bernhard A. “Product Liability 2.0- Mere Update or New Version?.” In *Liability for Artificial Intelligence and the Internet of Things. Münster Colloquia on EU Law and the Digital Economy*, Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer, 99-116. Baden Baden: Nomos Verlag- Hart Publishing, 2019.

Koziol, Helmut. “Punitive Damages- A European Perspective.” *Lousiana Law Review* 6,3 (2008): 741-764

KPMG. *After the rainfall of IoT regulations*. Accessed 31 January 2023. https://advisory.kpmg.us/articles/2020/rainfall-iot-regulations.html.

Kranz, Gerry. “Technological Convergence.” *Tech Target*. Accessed 31 January 2023. https://www.techtarget.com/searchdatacenter/definition/technological-convergence.

Kuan Hon, W., Christopher Millard, and Ian Walden. “The problem of 'personal data' in cloud computing: What information is regulated? the cloud of unknowing.” *International Data Privacy Law* 1,4 (2011):211-228. https://dx.doi.org/10.1093/idpl/ipr018.

Lachance, Jocelyn. “Sommes-nous égaux face aux écrans en période de confinement?.” *The Conversation*. April 19, 2020. Accessed 31 January 2023. https://theconversation.com/sommes-nous-egaux-face-aux-ecrans-en-periode-de-confinement-136130.

Landes, William M., and Richard A. Posner. *The Economic Structure of Intellectual Property Law*. Cambridge-Massachusetts, London-England; 2004.

Lauer Madelyn, Jordan P. Barker, Mitchell Solano, and Dubin Jonathan. “FDA Device Regulation,” *Missouri Medecine* 114,4(2017): 283-288.

Lee, Joong Hee., Yong Min Kim, Ilsun Rhiu, and Myung Hwan Yun. “A Persona-Based Approach for Identifying Accessibility Issues in Elderly and Disabled Users’ Interaction with Home Appliances.” *Applied Sciences* 11,1(2021): 368. https://dx.doi.org/10.3390/app11010368.

Leenes, Ronald, and Silvia De Conca. “Artificial intelligence and privacy- AI enters the house through the Cloud.” In *Research Handbook on the Law of Artificial Intelligence*, Woodrow Barfield, Ugo Pagallo, 285-306. Chelthenam: Edgar Elgar publishing 2018

Lemley, Mark, and Bryan Casey. “Remedies for Robots”. *The University of Chicago Law* Review 86(2018): 1311-1396.

“Lenovo tailors horizon table-pc for the home with three fashionable furniture designs.” *Lenovo story hub*. May 15, 2013. Accessed 31 January 2023. https://news.lenovo.com/pressroom/press-releases/lenovo-tailors-horizon-table-pc-for-the-home-with-three-fashionable-furniture-designs/.

Lenze, Stefan. “German product liability: between European directives, American Restatments and common sense,” In *Product Liability in Comparative Perspective*, Duncan Fairgrieve, 102-137. Cambridge: Cambridge University Press, 2005.

Le Pailleur, Félix., Bo Huang, Pierre-Majorique Léger, and Sylvain Sénécal. " A New Approach To Measure User Experience with Voice-Controlled Intelligent Assistants: A Pilot Study." In *Human-Computer Interaction. Multimodal and Natural Interaction. HCII 2020. Lecture Notes in Computer Science*(), vol 12182. Kurosu, M., 197-208. Cham, Switzerland :Springer Cham, 2020.

Lerman, Rachel. and Shaban, Hamza. "Amazon will see you now: Tech giant buys health-care chain for $3.9 billion." *The Washington Post.* 21 July 2022.Accessed 31 January 2023. https://www.washingtonpost.com/business/2022/07/21/amazon-health-care/ .

Li, Ming, and Zhonggen Yu. "Teachers' Satisfaction, Role, and Digital Literacy during the COVID-19 Pandemic." *Sustainability* 14,3(2022):1121, https://dx.doi.org/10.3390/su14031121.

Lilienthal, Jesse W. "Privity of Contract." *Harvard Law Review* 1, 5 (1887): 226-232.

Lior, Anat. "The AI Accident Network: Artificial Intelligence Liability Meets Network Theory," *Tulane Law Review* 95, 2020. Available at SSRN: 1-58**,** Accessed 31 January 2023, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3561948

Llwelyn, Karl N. "On Warranty of Quality and Society," *Columbia Law Review* 36,5(1936): 699-744.

Lohachab, Ankur, Anu , Lohachab, and Ajay Jangra. "A comprehensive survey of prominent cryptographic aspects for securing communication in post-quantum IoT networks." *Internet of Things* 9 (2020): 100174. https://dx.doi.org/10.1016/j.iot.2020.100174.

Lohsse, Sebastian, Schulze, Reiner and Staudenmayer, Dirk (eds.). *Liability for Artificial Intelligence and the Internet of Things Münster Colloquia on EU Law and the Digital Economy IV*. Baden-Baden: Nomos, 2020.

Lutkevich, Ben. "What is Transmission Control Protocol (TCP?." *TechTarget*. October 2021. https://www.techtarget.com/searchnetworking/definition/TCP.

Luzak, Joasia. "A broken notion: Impact of modern technologies on product liability," *European Journal of Risk Regulation* 11,3 (2020):630-649.

Mach, Pavel and Becvar Zdenek. "Mobile Edge Computing: A Survey on Architecture and Computation Offloading." *IEEE Communications Surveys and Tutorials* 19,3 (2017):1628-1630. https://dx.doi.org/10.1109/COMST.2017.2682318.

Machnikowski, Piotr. "Product Liability for Information products?: The CJEU Judgment in VI / KRONE - Verlag Gesellschaft mbH & Co KG, 10 June 2021 [C-65/21]." *European Review of Private Law* 1(2022):191-200. "Conclusions." In *European Product Liability: An Analysis of the State of the Art in the Era of New Technologies*, Piotr Machnikowski, 669-705. Antwerp-Cambridge-Portland: Intersentia, 2016.

Magnus, Ulrich. "Product Liability in Germany."In *European Product Liability: An Analysis of the State of the Art in the Era of New Technologies*, Piotr Machnikowski, 237-274. Cambridge, Portland Antwerp: Intersentia, 2016.

"Magnuson-Moss Warranty Act."

Wikipedia. Accessed 31 January 2023. https://en.wikipedia.org/wiki/Magnuson%E2%80%93Moss_Warranty_Act

Marlin, Chris "How Covid-19 will change the way we design our homes," *World Economic Forum*. August 3, 2020. Accessed 31 January 2023. https://www.weforum.org/agenda/2020/08/how-covid-19-will-change-what-we-call-home-ddfe95b686/.

Markesinis Basil. S.(Sir). *The German Law of Obligations. Volume II. The Law of Torts: A Comparative Introduction*. Oxford: Clarendon Press, 1997.

Martín-Casals, Miquel, and Solé Feliu Josep. "Product Liability in Spain." In *European Product Liability: An Analysis of the State of the Art in the Era of New Technologies*, Piotr Machnikowski, 408-458. Cambridge, Portland, Antwerp: Intersentia, 2016.

Martinelli, Silvia. “La responsabilità delle piattaforme di intermediazione.” In *LA RESPONSABILITÀ CIVILE NELL’ERA DIGITALE (Atti della Summer school 2021),* Valentina V. Cuocci, Francesco Paolo Lops, Cinzia Motti, 267-282. Bari: Cacucci editore, 2022.

Marwedel, Peter. *Embedded System Design. Embedded systems, foundations of cyber-physical systems, and the Internet of Things.* Cham: Springer Cham, 2018. https://link.springer.com/book/10.1007/978-3-319-56045-8

Mazzamuto, Salvatore. *La responsabilità contrattuale nella prospettiva europea*. Torino: Giappichelli, 2015.

Mell Peter, and Timothy Grance for NIST. *The NIST Definition of Cloud Computing.* 2011. Accessed 31 January 2023, http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf.

Meroli, Stefano. “Design and implementation of Active Pixel Sensors (APS).” Stefano Meroli. Life of an Engineer at CERN. Accessed 31 January 2023. https://meroli.web.cern.ch/lecture_activepixelsensors.html.

Micklitz, Hans-W. “Risk, Tort and Liability.” In *New Private Law Theory*, Stefan Grundmann, Hans-W. Micklitz and Moritz Renner, 272-297. Cambridge: Cambridge University Press, 2021.

Minoli, Daniel, and Benedict Occhiogrosso. “Blockchain mechanisms for IoT security.” *Internet of Things* 1-2 (2018):1-13. https://dx.doi.org/10.1016/j.iot.2018.05.002

Ministero dello Sviluppo Economico (MISE). “*Proposte per Una Strategia italiana per l’intelligenza artificiale.”* MISE website. Accessed 31 January 2023. https://www.mise.gov.it/images/stories/documenti/Proposte_per_una_Strategia_italiana_AI.pdf.

Montagnani, Maria Lillà. ”La libera circolazione dei dati al bivio. Tra tutela dei dati personali e promozione dell’intelligenza artificiale europea.” *Mercato Concorrenza Regole* 2 (2019): 310

293-313. https://dx.doi.org/10.1434/95581.

Morais Carvalho, Jorge. “Country Reports: The Implementation of the EU Directives 2019/770 and 2019/771 in Portugal.” *Journal of European Consumer and Market Law* 11,1(2022):31-34. “Sale of Goods and Supply of Digital Content and Digital Services – Overview of Directives 2019/770 and 2019/771.” Journal of European Consumer and Market Law 2,5 (2019):194- 201.

Mordor Intelligence, INTERNET OF THINGS (IO) MARKET- GROWTH, TRENDS, COVID 19 IMPACT AND FORECASTS (2021-2026) https://www.mordorintelligence.com/industry-reports/internet-of-things-moving-towards-a-smarter-tomorrow-market-industry.

“Motor Insurance.” *Insurance Europe*, Accessed 31 January 2023. https://www.insuranceeurope.eu/priorities/20/motor-insurance.

Mozilla, Web of Things, website, Accessed 31 January 2023, https://iot.mozilla.org/gateway/ .

Nallapeni Manoji, Kumar and Kumar Mallick Pradeep. “The Internet of Things: Insights into the building blocks, component interactions, and architecture layers.” *Procedia Computer Science* 132 (2018): 109-117 https://doi.org/10.1016/j.procs.2018.05.170.

“Nebraska mother, teenager face charges in teens abortion after police obtain their Facebook DMs”, *CBS Bay Area- Technology*, August 10, 2022, https://www.cbsnews.com/sanfrancisco/news/facebook-nebraska-abortion-police-warrant-messages-celeste-jessica-burgess-madison-county/.

Neerhof Richard. “The Use of Conformity Assessment of Construction Products by the Eurppean Union and National Governments: Legitimacy, Effectiveness and the Functioning of the Union Market,”in *Certification, Trust, Accountability*, Peter Rott, 73 -106. Cham: Springer Nature Switzerland, 2019.

New Bauhaus Initiative. Accessed 31 January 2023. https://europa.eu/new-european-bauhaus/index_en.

“New legislative framework.” *European Commission*. Accessed 31 January 2023. https://ec.europa.eu/growth/single-market/goods/new-legislative-framework_en.

Nicolao, Lorenzo. " Realtà virtuale, crescono gli incidenti domestici: TV rotte, infortuni e 'braccio del gorilla'." *Corriere della Sera-LOGIN: TecnologiaInnovazione.* February 15, 2022. Accessed 31 January 2023. https://www.corriere.it/tecnologia/22_febbraio_15/realta-virtuale-crescono-incidenti-domestici-tv-rotte-infortuni-braccio-gorilla-2ed9360a-8e45-11ec-a91e-e98defcaa657.shtml.

Noto La Diega, Guido. *Internet of Things and the Law. Legal Strategies for Consumer-Centric Smart Technologies*. London: Routledge, 2022.

Ohm, Paul. "Broken promises of privacy: Responding to the surprising failure of anonymization," *UCLA Law Review* 57,6 (2010):1701-1777.

Olin, Andy. "How will COVID-19 alter today's house of tomorrow." *Rice Kinder Institute for Urban Research*. January 4, 2021. Accessed 31 January 2023. https://kinder.rice.edu/urbanedge/2021/01/04/Covid-19-trends-home-design-pandemic-work-from-home.

Oliphant, Ken, and Vanessa Wilcox. "Product Liability in England and Wales." In *European Product Liability: An Analysis of the State of the Art in the Era of New Technologies*, Piotr Machnikowski, 173-204. Cambridge, Portland Antwerp: Intersentia, 2016.

Orsekovic, Alexei. " Google to acquire Nest for $3.2 billion in cash." *Reuters*, January 13, 2014. https://www.reuters.com/article/us-google-nest-idUSBREA0C1HP20140113.

Osservatorio Internet of Things, *L'Internet of Things alla prova dei fatti: il valore c'è e si vede!* Milano: Politecnico di Milano 1863 School of Management and osservatori.net digital innovation, 2021.

Osservatorio Povertà Educativa-Openpolis- Con i Bambini. *Disuguaglianze digitali. Bambini e famiglie tra possibilità di accesso alla rete e dotazioni tecnologiche nelle scuole*. 2020. Accessed 31 January 2023. https://www.openpolis.it/wp-content/uploads/2020/07/Disuguaglianze-digitali.pdf.

Owles Derrick, and Worsdall Anthea. *Product Liability Casebook. US and UK judgments and commentaries*. Cholchester; Lloyd's of London Press Ltd, 1984.

Oxford Internet Institute. "Press Release- AI modelling tool developed by Oxford Academics incorporated into anti-bias software." Accessed 31 January 2023. https://www.oii.ox.ac.uk/news-events/news/ai-modelling-tool-developed-by-oxford-academics-incorporated-into-amazon-anti-bias-software-2/.

Pagallo Ugo, Durante Massimo, and Monteleone Shara. "What is New with the Internet of Things in Privacy and Data Protection? Four Legal Challenges on Sharing and control IoT." in *Data Protection and Privacy: (In) visibilities and infrastructures*, Ronald Leenes, Rosamunde van Brakel Serge Gutwirth and Paul De Hert,59-78. Cham: Springer, 2017. https://link.springer.com/book/10.1007/978-3-319-50796-5#about .

Parchomovsky, Gideon, and Alex Stein. "Torts and Innovation." *Michigan Law Review* 107,2(2008): 286-316.

Pasquale, Frank. *New Laws of Robotics- Defending Human Expertise in the Age of AI*. Cambridge Massachusetts & London, England: the Belknap Press of Harvard University Press, 2020; *The Black Box Society*. Cambridge-Massachusetts, London-England: Harvard University Press, 2015.

Patent Progress. "Too many patents." Accessed 31 January 2023.https://www.patentprogress.org/systemic-problems/too-many-patents/.

Paulovich, Fernando V., Maria Cristina F. De Oliveira, and Osvaldo N. Oliveira Jr. "A Future with Ubiquitous Sensing and Intelligent systems," *ACS Sens* 2018, 1433-1438 https://pubs.acs.org/doi/pdf/10.1021/acssensors.8b00276

Peel Edween, and Goudkamp James. *Winifield Jolowicz Tort*. London: Thomson Reuters-Sweet&Maxwell, 2014, 19th ed

Pentheroudakis, Chryssoula, and Justus Baron. *Licensing Terms of Standard Essential Patents. A Comprehensive Analysis of Cases.* Luxembourg: JRC, 2017. https://dx.doi.org/10.2791/32230.

Perry, Susa,n and Roda, Claudia. “The Internet of Things,” in *Human Rights and Digital Technology*. *Digital Tightrope*, Susan Perry and Claudia Roda, 131-162. London: Palgrave Mc Millan,2017. https://link.springer.com/book/10.1057/978-1-137-58805-0.

Phan, Lin-An, and Kim Taehong. “Breaking down the compatibility problem in Smart Homes. A Dynamically Updatable Gateway Platform.” *Sensor* 20,10 (2020): 2873. https://dx.doi.org/10.3390/s20102783.

Phillips, Jerry J. and Pryor, Robert E. *Products Liability Volume I*. Wolters Kluwer Products Liability Library, 1993, 2nd ed.

Podszun Rupprecht, Philipp Bongartz and Sarah Langestein. “The Digital Markets Act: Moving from Competition Law to Regulation for Large Gatekeepers.” *Journal of European Consumer and Market Law* 2(2021): 60-67.

Posner, Richard A. “The Concept of Corrective Justice in Recent Theories of Tort Law”. *The Journal of Legal Studies* 10,1(1981): 187-206.

Poumarède, Matthieu, and Philippe le Toruneau. “Chapitre 6312- Domaine de la responsabilité.” In *Droit de la Responsabilité et des contrats*, Philippe le Toruneau, 2576-2586. Dalloz: Paris, 2021-2022,12 th ed.

Preece, Jenny, Kim McKee, David Robinson and John Flint. “Urban rhythms in a small home: COVID-19 as a mechanism of exception.” *Urban Studies* (2021): 2. https://dx.doi.org/10.1177/00420980211018136.

Progin-Theuerkauf, Sarah and Melanie Berger. “ECJ Confirms Validity of the Rule of Law Conditionality Regulation.” *European Law Blog*. March, 11 2022. Accessed 31 January 2023. https://europeanlawblog.eu/2022/03/11/ecj-confirms-validity-of-the-rule-of-law-conditionality-regulation/.

Prosser, William L. “The Assault upon the Citadel (Strict Liability to the Consumer).” *Yale Law Journal* 69,7(1960): 1099-1148.

Purtova, Nadezhda. “The law of everything. Broad concept of personal data and future of EU data protection law.” *Law Innovation and Technology* 10,1 (2018):40-81. https://dx.doi.org/10.1080/17579961.2018.1452176.

Pwc. *Emerging Trends in Real Estate ®: Europe 2022*, Accessed 31 January 2023, https://www.pwc.com/gx/en/industries/financial-services/asset-management/emerging-trends-real-estate/europe-2022.html.

Pwc. “Three actions for IoT device manufacturers from the IoT Cybersecurity Improvement Act of 2020.” Accessed 31 January 2023. https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/iot-cyber-improvement-act.html.

Quaglio, Gianluca. *Environmantal Impacts of the 5G. EPRS study.* Brussels: European Parliament, 2021. .https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690021/EPRS_STU(2021)690021_EN.pdf.

Quintarelli, Stefano. *Capitalismo immateriale*. Torino: Bollati Boringhieri, 2019.

Rachum-Twaig, Omri. “Whose Robot is it Anyway? Liability for Artificial Intelligence Based Robots.” *University of Illinois Law Review* 4(2020): 1143-1176.

Rainey, Toria. “Is Breaking Up Amazon, Facebook, and Google a Good Idea?.” *Boston University Today*, October 7, 2019. https://www.bu.edu/articles/2019/break-up-big-tech/.

Rajneri, Eleonora. “Country Reports: Product Liability in Italy,” *Journal of European Consumer and Market Law* 5(2019): 209-212.

Reed, Chris. *Internet Law. Text and Materials, second edition.* Cambridge: Cambridge University Press, 2004.

“Reform of the Product Liability Directive.” *ELI website*. Accessed 31 January 2023. https://europeanlawinstitute.eu/projects-publications/current-projects/current-projects/pld/.

Reich, Norbert. “Free Movement v. Social Rights in an Enlarged Union - the Laval and Viking Cases before the ECJ.” *German Law Journal* 9, 2(2008): 125-161.

Reimann, Mathias. “Liability for Defective Products at the beginning of the Twenty First Century: Emergence of a Worldwide standard?.” *The American Journal of Comparative* Law 51,4(2003):751-838. https://www.jstor.org/stable/3649130.

Ricolfi, Marco. “Il futuro della proprietà intellettuale nella società algoritmica,” *Giurisprudenza Italiana*, (2019): 10-36.

Riefa, Christine, and Harriet Gamper. “Economic theory and consumer vulnerability. Exploring an uneasy relationship” In *Vulnerable Consumers and the Law. Consumer Protection and Access to Justice*, Christine Riefa and Séverine Saintier 17-30. London and New York: Routledge, 2021.

Rinaldi, Manuela. “RESPONSABILITÀ OGGETTIVA IN GENERALE.” In *Trattati Giuridici Omnia-La Responsabilità Civile, vol. III* ., Paolo Cendon, 3539-3583. Torino: Utet Giuridica, 2020, 2nd ed.

Robins, Kevin and Mark Hepworth. “Electronic spaces: new technologies and the future of cities. ”*Futures* 20,2 (1989): 155-176.

Rodotà, Stefano. “Dichiarazione dei Diritti di Internet.” Camera dei Deputati. Accessed 31 January 2023. https://www.camera.it/application/xmanager/projects/leg17/commissione_internet/dichiarazione_dei_diritti_internet_pubblicata.pdf; *Il Problema della Responsabilità Civile.* Milano: Giuffrè, 1964.

Romkey, John, “The Toast of the IoT. The 1990 interop Internet toaster.” *IEEE Consumer Electronics magazine* 6, 1 (2017): 116-119, https://dx.doi.org/10.1109/MCE.2016.2614740.

Rossi, Arianna, and Monica Palmirani. “DAPIS: An ontology-based data protection icon set,” in *Frontiers in the Artificial Intelligence Applications*, Ginevra Peruginelli and Sebastiano Faro, 181-195. Amsterdam: IoS press, 2019.

Rotman David. ”We are not prepared for the end of Moore’s Law”, *MIT Technology Review*, February 24, 2020. Accessed 31 January 2023. https://www.technologyreview.com/2020/02/24/905789/were-not-prepared-for-the-end-of-moores-law/.

Routray, Sudhir K. and K.P. Sharmila. “Green Initiatives in 5G,” in *Proceeding of IEEE - 2nd International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics, IEEE - AEEICB 2016* (Chennai,India, 2016) : 619-620. https://dx.doi.org/10.1109/AEEICB.2016.7538363.

Rudin, Cynthia, and Joanna Radin. “Why Are We Using Black Box Models in AI When We Don’t Need To? A lesson From an Explainable AI Competition”. *Harvard Data Science Review* 1,2 (2019). https://doi.org/10.1162/99608f92.5a8a3a3d.

Saint, Simon. “AD-APT: How will buildings adapt to the new realities of home?.” *Woods- Bagot Journal*. Accessed 31 January 2023. https://www.woodsbagot.com/journal/ad-apt-how-will-buildings-adapt-to-the-new-realities-of-home-as/ .

“Safety Best Practices for IoT Devices.” *Practical Law (Westlaw)* (2019):1-14.

Satyajit, Sinha. “State of IoT 2021: Number of connected IoT devices growing 9% to 12.3 billion globally, cellular IoT now surpassing 2 billion.” *IoT Analytics*. 22 September 2021, Accessed 31 January 2023. https://iot-analytics.com/number-connected-iot-devices/.

Schuilenburg, Marc, and Rik Peeters. “The Algorithmic Society. An Introduction.” In *The Algorithmic Society. Technology, Power and Knowledge*, Marc Schuilenburg and Rik Peeters,1-15. Routledge:London, 2020 .https://dx.doi.org/10.4324/9780429261404

Schülze, Reiner and Fryderyk Zoll. *European Contract Law*, 3rd ed. Baden-Baden: Beck-Hart-Nomos, 2021.

Schwartz, Victor E., Kathryn Kelly, and David F. Partlett. *Prosser Wade and Schwartz’s Torts. Tenth edition*. New York: Foundation Press,2000.

Schweblin, Samantha. *Kentuki*. Rome: SUR,2019. Italian translation from Spanish.

Sein, Karin. “Interplay Of Digital Content Directive, European Electronic Communications Code And Audiovisual Media Directive In Communications Sector,” 12,1 (2021) 169-180; “What Rules Should Apply to Smart Consumer Goods?”; “Goods with Embedded Digital Content in the Borderland Between the Digital Content Directive and “ Normal “ Contract Law” *JIPITEC* 8 (2017): 96-110.

Sein, Karin and Spindler Gerard. “The new Directive on Contracts for theSupply of Digital Content and Services- Scope of Application and Trader’s Obligation to supply-Part 1.” *European Review of Contract Law* 15,3 (2019):257-279. https://dx.doi.org/10.1515/ercl-2019-0016.

“Sensors and Smart Home.” *IBM*. December 15, 2016. Accessed 31 January 2023. https://www.ibm.com/blogs/internet-of-things/sensors-smart-home/.

Serrenho, Tiago, and Bertoldi, P. *Smart home and appliances: State of the art. Energy, Communications, Protocols and Standards*. Luxembourg: JRC, 2019.

Sethi, Pallavi, and Sarangi Smruti R. “Internet of Things: Architectures, Protocols, and Applications.” *Journal of Electrical and Computer Engineering* (2017) https://dx.doi.org/10.1155/2017/9324035

Shabandri, Bilal, and Piyush Maheshwri. “Enhancing IoT Security and Privacy Using Distributed Ledgers with IOTA and the Tangle.” In *2019 6th International Conference on Signal Processing and Integrated Networks (SPIN) Enhancing* (2019): 1069-1075. https://dx.doi.org/10.1109/SPIN.2019.8711591

Shafique, Kinza., Bilal A. Khawaja, Farah Sabir, Sameer Qazi, and Muhammad Mustaqim. “Internet of things (IoT) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5G-IoT Scenarios.” *IEEE Access* 8 (2020): 23022-23040. https://dx.doi.org/10.1109/ACCESS.2020.2970118.

Shasha, Sharon, Moustafa , Mahmoud, Mohammad Mannan, and Amr Youssef. “Playing With Danger: A Taxonomy and Evaluation of Threats to Smart Toys.” *IEEE Internet of Things Journal* 6, 2(2019): 2986-3002. https://dx.doi.org/10.1109/JIOT.2018.2877749.

Shavell, Steven. *Foundations of Economic Analysis of the Law*. Cambridge, Massachussets - London: The Belknap Press of Harvard University Press, 2004.

Shead, Sam. “Amazon Echo and Google Home owners spied on by apps,” *BBC News Tech*, October 21, 2019, Accessed 31 January 2023, https://www.bbc.com/news/technology-50124713.

Sicari, Sabrina, Alessandra Rizzardi, and Alberto Coen-Porisini. “5G In the internet of things era: An overview on security and privacy challenges.” *Computer Networks* 179 (2020): 107435.

Sigg, Stephan, Kai Kunze, and Xiaoming Fu. “Recent Advances and Challenges in Ubiquitous Sensing” *PIEE* (2015) https://arxiv.org/abs/1503.04973 .

Sikken, Arianne. “General product safety regulation: Council adopts its position,” *European Council website-press release*. 20 July 2022. Accessed 31 January 2023. https://www.consilium.europa.eu/en/press/press-releases/2022/07/20/general-product-safety-regulation-council-adopts-its-position/

Simpson, Robin. “A universal perspective on vulnerability. International definitions and targets.” In *Vulnerable Consumers and the Law. Consumer Prorection and Access to Justice*, Christine Riefa and Séverine Saintier, 31-50. London and New York: Routledge, 2021.

Sixsmith, Andrew, and Gloria Gutman. *Technologies for Active Ageing.* New York, Heidelberg, Dodrecht, London: Springer 2013.

Social and Economic Committee. “Opinion of the Social and Economic Committee on the EC proposal on the regulation of AI, COM 205/2021 final.” EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021AE2456.

Solove Daniel. “Introduction: Privacy Self-Management and the Consent Dilemma,” *Harvard Law Review* 126,7 (2013): 1880-1903.

Solove Daniel J., and Woodrow Hartzog. “The FTC and the New Common Law of Privacy.” *Columbia Law Review* 114, 3(2014):583-676.

Solove, Daniel, and Paul M. Schwartz. *Information Privacy Law*. Netherlands: Wolters Kluwer, Aspen Casebook series, 6th edition.

Sovacool Benjamin K., and Dylan D. Furszyfer Del Rio. “Smart home technologies in Europe : A critical review of concepts , benefits , risks and policies.” *Renewable and Sustainable Energy Reviews* 120 (2019): 109663 https://doi.org/10.1016/j.rser.2019.109663.

“Smart Home. La Casa Intelligente”, *Il Giornale dell’architettura*, Accessed 31 January 2023.

https://ilgiornaledellarchitettura.com/2021/09/01/smart-home-la-casa-intelligente/.

Stankowska, Anna, and Izabela Stankowska-Mazur. “The Third Wave of COVID-19 versus the Residential Preferences in Poland: An Assessment of Economic Factors and Psychological Determinants.” *Sustainability* 14,3(2022):1339. https://dx.doi.org/10.3390/su14031339.

Strengers, Yolande. *Smart Energy Technology in Everyday Life. Smart Utopia*. London: Palgrave Macmillan, 2013. https://dx.doi.org/10.1057/9781137267054.

Study Group on a European Civil Code and the Research Group on Private Law (Acquis Group) *Draft Common Frame of Reference*. Munich: Sellier, 2009. https://www.law.kuleuven.be/personal/mstorme/2009_02_DCFR_OutlineEdition.pdf.

Taddeo, Mariarosaria. “Modelling trust in artificial agents, a first step toward the analysis of e-trust.” *Minds & Machines* 20,2(2010): 243-257. https://dx.doi.org/10.1007/s11023-010-9201-3.

Taliadoros, Jason. “The Roots of Punitive Damages at Common Law: A longer History”. *Cleveland State Law Review* 64,2 (2016) 251-302.

Tartaglione, Enzo. *IT for beginners*, Lecture materials, University of Turin, September- October 2020.

Terrell, Hanna Katie. “Transceiver.” *TechTarget*. September 2021. https://www.techtarget.com/searchnetworking/definition/transceiver

Terryn, Evelyne. “A Right to Repair? Towards Sustainable Remedies in Consumer Law.” *European Review of Private Law* 4 (2019): 851-873. “The New Consumer Agenda : A Further Step Toward Sustainable Consumption?.”*Journal of Consumer and Market Law* 10,1 (2021): 1-3.

The Onlife Initiative. “The Onlife Manifesto.” In *The Onlife Manifesto: Being Human in a Hyperconnected Era*, Luciano Floridi, 1-13. Cham, Switzerland: Springer, 2015.

“Therac 25.” *Wikipedia*. Accessed 31 January 2023, https://en.wikipedia.org/wiki/Therac-25.

Thobani, Shaira. “Il Danno Non Patrimoniale Da Trattaemento Illecito dei Dati Personali (Estratto).” *Diritto dell’Informazione e dell’Informatica*. (2017): 452-455.

Tieglaar, Leonike. “How to Sanction a Breach of Information Duties of the Consumer Rights Directive?.” *European Review of Private Law*, 27 1 (2019): 25-57.

Tilley, Aaron. “How Hackers Could Use A Nest thermostat As An Entry Point Into Your Home.” *Forbes*. March 6, 2015.for https://www.forbes.com/sites/aarontilley/2015/03/06/nest-thermostat-hack-home-network/.

TiMOTION. The role of electric actuation in smart homes. Accessed 31 January 2023. https://www.timotion.com/en/news/news_content/news-and-articles/comfort-motion/the-role-of-electric-actuation-in-smart-homes?upcls=1481189409&guid=1529663363.

Tomás, Juan Pedro. “What is an IoT gateway?,” *Enterprise IoT insights*. 2017. Accessed 31 January 2023, https://enterpriseiotinsights.com/20170517/internet-of-things/20170517internet-of-thingswhat-iot-gateway-tag23-tag99.

Tommasi, Sara. “The Liability of Internet Service Providers in the Proposed Digital Services Act.” *European Review of Private Law* 6(2021): 925-944.

Tosi, Emilio. *Responsabilità Civile per Illecito Trattamento dei Dati Personali e Danno non patrimoniale. Oggettivazione del Rischio e Riemersione del Danno Morale con Funzione Deterrente e Sanzionatoria.* Milano: Giuffrè Francis Lefebre, 2019.

Tovo, Carlo. “Judicial Review of Harmonised Standards: Changing the Paradigms of Legality and Legitimacy of Private Rulemaking under EU Law,” *Common Market Law Review* 55 (2018):1187-1216.

Tran, Alexander H. “The Internet of Things and potential remedies in privacy tort law,” *Columbia Journal of Law and Social Problems* 50,2 (2017):263-298.

Tridimas, Takis. “The Principle of Proportionality.” In *Oxford Principles of European Union Law: The European Legal Order: Volume I*, Robert Schütze and Takis Tridimas, 243-246. Oxford: Oxford University Press, 2018. https://dx.doi.org/10.1093/oso/9780199533770.003.0010.

Tridimas, Takis, and Napoleon Xanthoulis. "A Legal Analysis of the Gauweiler Case." in "The European Court of Justice, the European Central Bank and the Supremacy of EU Law” Federico Fabbrini, *Maastricht Journal of European & Comparative Law*, Special Issue 23, 1 (2016): 17-39. https://dx.doi.org/10.1177/1023263X1602300102.

Trimarchi, Pietro. *La Responsabilità Civile: Atti Illeciti, Rischio, Danno.* Milano: Giuffrè Francis Lefebre, 2019.

Tse, Crystal, and Jonathan Browning. “Locked-Down Lawyers Warned Alexa Is Hearing Confidential Calls.” *Bloomberg Law*. March 20, 2020. Accessed 31 January 2023, https://news.bloomberglaw.com/business-and-practice/locked-down-lawyers-warned-alexa-is-hearing-confidential-calls.

Tun, So Ye Yint., Samaneh Madanian and Frhaan Mirza. “Internet of things (IoT) applications for elderly care: a reflective review.” *Aging Clinical and Experimental Research* 33(2021):855-867.

Twigg-Flesner, Christian. “From REFIT to a rethink: time for fundamental EU Consumer Law reform.” *Journal of European Consumer and Market Law* 6(2017):185-189.

UNDP. *Sustainable Development Goals*. Accessed 31 January 2023. https://sdgs.un.org/goals.

Van Alsenoy, Brendan. *Data Protection Law in the EU: Rules Responsibilities and Liability*. Antwerp, Cambridge, Portland: Intersentia, 2019.

Van Dam, Cees. “Strict Liability.” In *European Tort Law*, Cees Van Dam, 297-306. Oxford: Oxford University Press, 2013.

van Gerven, Walter, Jeremy Lever, and Pierre Larouche. *Cases Materials and Text on National, Supranational and International TORT LAW.* Oxford and Portland, Oregon: Hart, 2000.

Varjovi, Ali Eslami, and Sharham Babaie. “Green Internet of Things (GIoT): Vision, applications and research challenges.” *Sustainable Computing: Informatics and Systems* 28 (2020):100448. https://dx.doi.org/10.1016/j.suscom.2020.100448.

Verbruggen Paul. “Tort Liability for Standards Development in the United States and European Union.” In *The Cambridge Handbook of Technical Standardization Law*, Jorge Contreras, 60-88. Cambridge: Cambridge University Press, 2019. https://dx.doi.org/10.1017/9781316416785.005.

Verheyen, Thomas. ”Full Harmonization, Consumer Protection and Products Liability: A Fresh Reading of the Case Law of the ECJ,” *European Private Law Review* 26(2018): 119-140.

Viney, Geneviève, and Patrice Jourdain. *Les Conditions de la Responsabilité 3e éd* In *Traité de Droit Civil*, Jaques Ghestin. Paris: LGDJ, 2006.

Viscusi, William Kip., and Michael J. Moore. “Product Liability, Research and Development.” *Journal of Political Economy* 101,1(1993):161-184.

Vizzoni, Lavinia. *Domotica e diritto. La Smart Home tra regole e responsabilità*. Milano: Giuffrè, 2021

Wagner, Kate. “Machines for Living In: How Technology Shaped a Century of Interior Design.” *99% Invisible*. January 13, 2017. Accessed 31 January 2023. https://99percentinvisible.org/article/machines-living-technology-shaped-century-interior-design/.

Wallerman, Anna. “Pie in the sky when you die? Civil liability of notified bodies under the Medical Devices Directive: *Schmitt”*. *Common Market Law Review* 55 (2018):265-278.

Watson, Bruce. “The troubling evolution of corporate greenwashing.” *The Guardian*. August 20, 2016. Accessed 31 January 2023. https://www.theguardian.com/sustainable-business/2016/aug/20/greenwashing-environmentalism-lies-companies.

Weatherill, Stephen. “The Limits of Legislative Harmonization Ten Years after Tobacco Advertising: How the Court ' s Case Law has become a ‘Drafting Guide’.” *German Law Journal* 12,3 (2011): 827-864.

Weber, Rolf H. “Internet of Things - Need for a New Legal Environment?.” *Computer Law and Security Review* 25, 6 (2009): 522-527. https://dx.doi.org/10.1016/j.clsr.2009.09.002.

Weiser, Mark. “The Computer for the 21st Century.” *Sci-Am*. 1991.

Wenderhorst, Christiane. “Strict Liability for AI and other Emerging Technologies,” *Journal of European Tort Law* 11,2 (2020):150-180. https://dx.doi.org/10.1515/jetl-2020-0140.

Werro, Franz, and Erdem Büyüksagis. “The bounds between negligence and strict liability.” In *Comparative Tort Law: Global Perspectives 2nd*, Mauro Bussani and Anthony J. Sebok 186-213. Cheltenham, UK & Northampton, USA: Edward Elgar Publishing, 2021.

Winston, Andrew. “Sustainable Business Went Mainstream in 2021.” *Harvard Business Law Review*. December 27, 2021. Accessed 31 January 2023. https://hbr.org/2021/12/sustainable-business-went-mainstream-in-2021.

Whittaker, Simon. “The Creation and Maintenance of the EEC Directive on Liability for Defective Products and the Process of its Implementation in the UK and France.” In *Liability for Products: English Law, French Law, and European Harmonization*, Simon Whittaker, 430-475. Oxford : Oxford University Press,2005.

Wuyts, Daily. “The Product Liability Directive- More than two Decades of Defective Products in Europe.” *Journal of European Tort Law* 5,1 (2014):1-3. https://dx.doi.org/10.1515/jetl-2014-0001.

Xanadu Houses, *Wikipedia*, Accessed 31 January 2023. https://en.wikipedia.org/wiki/Xanadu_Houses.

Yamazaki, Tatsuya. “The Ubiquitous Home,” *International Journal of Smart Home* 1,1 (2007): 17-18.

Zabeu, Sheila. “Amazon buys One Medical, subscription health services company.” *NETWORKKING. The IT Monitoring Magazine*. July 25, 2022. Accessed 31 January 2023. https://network-king.net/amazon-buys-one-medical-subscription-health-services-company/#:~:text=Amazon%20buys%20One%20Medical%2C%20subscription%20health%20services%20company,-Sheila%20Zabeu&text=After%20Oracle's%20largest%20acquisition%20completed,for%20another%20shot%20from%20Amazon

Zuboff, Shoshana. *The Age of Surveillance Capitalism: the Fight for a Human Future at the New Frontier of Power*. London: Profile Books, 2019.

2. EU legal acts (proposed and enacted)

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

OJ L 210, 7.8.1985, p. 29–33-" EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31985L0374. Hereinafter PLD.

"Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts

OJ L 95, 21.4.1993, p. 29–34." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52003DC0702. Hereinafter UTC.

"Directive 1995/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data *OJ L 281*, 23.11.1995, p. 31–50." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046.

"Directive 1999/44/EC of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees *OJ L 171, 7.7.1999*, p. 12–16." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31999L0044.

"Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)**,** *OJ L 178, 17.7.2000, p. 1–16*." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32000L0031.

"Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety (Text with EEA relevance) OJ L 11, 15.1.2002, p. 4–17." EUR-Lex. Accessed 31 January 2023 https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32001L0095.

"Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058.

"Directive 2004/35/CE of the European Parliament and of the Council of 21 April 2004 on environmental liability with regard to the prevention and remedying of environmental damage. OJ L 143, 30.4.2004, p. 56–75" EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32004L0035.

Hereinafter Environmental Liability Directive or ELD.

"Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (Unfair Commercial Practices Directive) (Text with EEA relevance)

OJ L 149, 11.6.2005, p. 22–39." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32005L0029&qid=1661804213957. Hereinafter UCPD.

"Directive 2009/103/EC of the European Parliament and of the Council of 16 September 2009 relating to insurance against civil liability in respect of the use of motor vehicles, and the enforcement of the obligation to insure against such liability (Codified version) (Text with EEA relevance) OJ L 263, 7.10.2009, p. 11–31." EURLEX. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32009L0103.

"Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council Text with EEA relevance *OJ L 304, 22.11.2011*, p. 64–88." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32011L0083&qid=1661353206931. Hereinafter CRD

"Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives

94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council Text with EEA relevance

OJ L 316, 14.11.2012, p. 12–33." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32012R1025.

"COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A Digital Single Market Strategy for Europe, COM/2015/0192 final." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192.

"COMMISSION STAFF WORKING DOCUMENT GUIDANCE ON THE IMPLEMENTATION/APPLICATION OF DIRECTIVE 2005/29/EC ON UNFAIR COMMERCIAL PRACTICES Accompanying the document COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A comprehensive approach to stimulating cross-border e-Commerce for Europe's citizens and businesses SWD/2016/0163 final." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52016SC0163.

"Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) *OJ L 119, 4.5.2016,* p. 1–88." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679&qid=1661353452590.

"Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) COM/2017/010 final - 2017/03 (COD)." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010.

"Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (Text with EEA relevance) *OJ L 157,* 15.6.2016, p. 1–18," EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0943.

"Medical Device Regulation (MDR) Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Text with EEA relevance.) *OJ L 117, 5.5.2017, p. 1–175,"* EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R0745. Hereinafter MDR.

"Directive (EU) 2018/844 of the European Parliament and of the Council of 30 May 2018 amending Directive 2010/31/EU on the energy performance of buildings and Directive 2012/27/EU on energy efficiency (Text with EEA relevance) PE/4/2018/REV/1*OJ L 156, 19.6.2018* p. 75–91. " EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L0844.

"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." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1807. Hereinafter Free Flow of Data Regulation, or FFDR.

"Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast)Text with EEA relevance.

PE/52/2018/REV/1 *OJ L 321, 17.12.2018*, p. 36–214.*"* EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2018.321.01.0036.01.ENG. Hereinafter EECC.

"REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL AND THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE on the Application of the Council Directive on the

approximation of the laws, regulations, and administrative provisions of the Member States concerning liability for defective products (85/374/EEC) COM/2018/246 final," 2, EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52018DC0246.

"COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Artificial Intelligence for Europe COM/2018/237 final." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN.

"COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Coordinated Plan on Artificial Intelligence COM/2018/795 final." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:795:FIN

REFIT Scoreboard. Accessed 31 January 2023. https://op.europa.eu/webpub/com/refit-scoreboard/en/policy/11/index.html.

"Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services (Text with EEA relevance.) PE/26/2019/REV/1*OJ L 136, 22.5.2019,* p. 1–27." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32019L0770. Hereinafter, SDG

"Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC (Text with EEA relevance.)

PE/27/2019/REV/1*OJ L 136, 22.5.2019,* p. 28–50," EUR-Lex. Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32019L0771. Hereinafter, DCDS.

"Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules (Text with EEA relevance) PE/83/2019/REV/1 *OJ L 328, 18.12.2019,* p. 7–28," EUR-Lex, Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32019L2161. Hereinafter Dir 2019/2161.

"COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS The European Green Deal, COM/2019/640 final." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2019%3A640%3AFIN.

"European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)) *OJ C 404, 6.10.2021, p. 107–128,*" EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020IP0276.

"COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Secure 5G deployment in the EU - Implementing the EU toolbox, COM/2020/50 final." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:0050:FIN.

"COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A Renovation Wave for Europe - greening our buildings, creating jobs, improving lives

COM/2020/662 final." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0662.

"COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Shaping Europe's digital future, COM/2020/67 final," EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0067&qid=1661352744218.

“REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL AND THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, COM(2020)64 final.” EUR-Lex. Accessed 31 January 2023.

https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1593079180383&uri=CELEX%3A52020DC0064.

“WHITE PAPER On Artificial Intelligence - A European approach to excellence and trust

COM/2020/65 final.” EUR-Lex. Accessed 31 January 2023.

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0065.

“COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A European strategy for data COM/2020/66 final.” EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066.

“COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL New Consumer Agenda Strengthening consumer resilience for sustainable recovery

COM/2020/696 final.” EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0696. Hereinafter, New Consumer Agenda.

“Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on contestable and fair markets in the digital sector (Digital Markets Act)

COM/2020/842 final.” EUR-Lex. Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A842%3AFIN .

“Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC

COM/2020/825 final.” EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN .

“Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTSCOM/2021/206 final, ”EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206&qid=1661352946581. Hereinafter AI Act or AIA.

“Regulation (EU) 2021/241 of the European Parliament and of the Council of 12 February 2021 establishing the Recovery and Resilience Facility *OJ L 57,* 18.2.2021, p. 17–75.” EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0241&qid=1661352828053.

“Commission Notice Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market.” Accessed 31 January 2023. https://ec.europa.eu/info/sites/default/files/c_2021_9320_1_ucpd-guidance_en.pdf .

“Commission Notice Guidance on the interpretation and application of Directive 2011/83/EU of the European Parliament and of the Council on consumer rights.”51-52. Accessed 31 January 2023. https://ec.europa.eu/info/sites/default/files/c_2021_9314_1_crd-guidance_en.pdf .

“Commission Staff Working Document. Accompanying the document REPORT FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT Final-Report- Sector inquiry into consumer Internet of Things (COM(2022)19 final) , Brussels, 20.1 2022, SWD(2022) 10 final. 89”. EUR-Lex. Accessed 31 January 2023. Commission Staff Working Document Accompanying the Document REPORT FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT Final report- Sector inquiry into consumer Internet of Things, SWD/2022/10 fina.l” EUR-Lex. Accessed 31 January 2023. https://eur-

lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022SC0010&qid=1653852206944. Hereinafter, Staff Working Document- Report on the Consumer IoT.

"European Declaration on the Digital Rights and Principles for the Digital Decade. COM/2022/28 final." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A28%3AFIN. Hereinafter, Charter for Digital Rights.

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (Data Act)

COM/2022/68 final." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN. Hereinafter DA.

"Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance) PE/85/2021/REV/1 *OJ L 152, 3.6.2022, p. 1–44*." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868. Hereinafter, DGA.

"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 COM/2022/454 final." EUR-Lex. Accessed 25 October 2022. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0454.

"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), Brussels, 28.9.2022 COM(2022) 496 final 2022/0303 (COD)." European Commission. Accessed 31 January 2023. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_5807.

"Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on liability for defective products, Brussels, 28.9.2022 COM(2022) 495 final 2022/0302 (COD)." EU Commission. Accessed 31 January 2023. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_5807.

"Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance) PE/17/2022/REV/1 OJ L 265, 12.10.2022, p. 1–66." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925&qid=1674037261043 .

"Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance) PE/30/2022/REV/1 *OJ L 277, 27.10.2022, p. 1–102*." EUR-Lex. Accessed 31October 2022. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=1666972131568.

"Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) PE/32/2022/REV/2, OJ L 333, 27.12.2022, p. 80–152." EUR-Lex. Accessed 18 January 2023. https://eur-lex.europa.eu/eli/dir/2022/2555 .

3. Conseil de l'Europe

Conseil de l'Europe. *Convention européenne sur la responsabilté du fait des produits en cas de lésions corporelles ou de décès*. Strasbourg, 27 January 1977. Accessed 31 January 2023. https://rm.coe.int/1680077328.

4. US Planned and Enacted Bills, Restatements and Policy Documents

American Law Institute. *Restatement of the Law Second Torts 2D, Volume 2*, *§§281-503.* Saint Paul, Minnesota: American Law Institute Publishers,1965.

"H.R. 11124- Medical Device Amendments, Sponsor: Rogers Paul g.,(1976)" Congress.gov., Accessed 31 January 2023. https://www.congress.gov/bill/94th-congress/house-bill/11124. Hereinafter Medical Amendments Act (MDA)

15 U.S.C.A. §45 Unfair methods of competition unlawful prevention by Commission, Westlaw.

"Children's Online Privacy Protection, (COPPA-1998), 15 U.S.C. §§ 6501-6506", *Code of Federal Regulation*. Accessed 31 January 2023.

https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312.

FTC Staff Report, *Internet of Things. Privacy and Security in a Connected World*. January 2015. Accessed 31 January 2023. https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

U.S. Department of Homeland Security. *Strategic Principles for Securing the Internet of Things Version 1.0*. November 15, 2016. Accessed 31 January 2023. https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf.

"Careful Connections: Keeping the Internet of Things Secure." *FTC*. Accessed 31 January 2023. https://www.ftc.gov/business-guidance/resources/careful-connections-keeping-internet-things-secure .

(California) "Senate Bill N 327 Chapter 886, An act to add Title 1.81.26 (2018)". Accessed 31 January 2023. https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.26.&part=4.&chapter=&article.

"H.R.1668 - IoT Cybersecurity Improvement Act of 2020, Sponsor Kelly Robin." Congress.gov. Accessed 31 January 2023, https://www.congress.gov/bill/116th-congress/house-bill/1668/text.

S.2992- American Innovation and Choice Online Act. Sponsor: Sen, Klobuchar,Amy, Senate, introduced 10/18/2021. Accessed 31 January 2023. https://www.congress.gov/bill/117th-congress/senate-bill/2992/text.

"U.S.- EU Trade and Technology Council Inaugural Joint Statement," *The White House*. September 29, 2021. Accessed 31 January 2023. https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/29/u-s-eu-trade-and-technology-council-inaugural-joint-statement/.

S.305-GOOD AI Act of 2021, Sponsor: Sen. Peters, Garty C. introduced 10/21/2021. Accessed 31 January 2023. https://www.congress.gov/bill/117th-congress/senate-bill/3035/text.

NIST. Consumer IoT Cybersecurity. Improving Consumer IoT Cybersecurity. Accessed 31 January 2023. https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/consumer-iot-cybersecurity.

NIST. *AI Risk Management Framework. Second Draft. August 18 2022*. Accessed 31 January 2023. https://www.nist.gov/system/files/documents/2022/08/18/AI_RMF_2nd_draft.pdf.

5. Cases

5.1. EU

"Plaumann & Co. v Commission of the European Economic Communities, Case C-25-62." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A61962CJ0025, hereinafter *Plaumann*.

"Internationale Handelsgesellschaft mbH v Einfuhr- und Vorratsstelle für Getreide und Futtermittel, Case C-11/70." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A61970CJ0011.

"Criminal proceedings against Bernard Keck and Daniel Mithouard, Cases C-267/91 and C-268/91." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A61991CJ0267.

"Brasserie du Pêcheur SA v Bundesrepublik Deutschland and The Queen v Secretary of State for Transport, ex parte: Factortame Ltd and others, Cases C-46/93 and C-48/93." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A61993CJ0046.

"Opinion of Advocate General Tesauro Commission of the European Communities v United Kingdom of Great Britain and Northern Ireland, Case C-300/95." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX:61995CC0300.

"Commission of the European Communities v United Kingdom of Great Britain and Northern Ireland, Case, C-300/95." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A61995CJ0300&qid=1659521422689. (Hereinafter *Commission v UK*).

"Federal Republic of Germany v European Parliament and Council of the European Union, Case C-376/98." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A61998CJ0376, hereinafter, *Tobacco Advertising I*.

"Opinion of Advocate General Ruiz-Jarabo Colomer, Henning Veedfald v. Århus Amstkommune C-203/99." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A61999CC0203&qid=1484153976108 .

"Henning Veedfald v. Århus AmstKommune, Case C-203/99." EUR-Lex. Accessed 31 January 2023.

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A61999CJ0203&qid=1659524361571, hereinafter *Veedfald*.

"Joined Opinion of AG Geelhoed delivered on 18 September 2001, Commission of the European Communities v French Republic, María González Sánchez v Medecina Asturiana." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX:62000CC0052. Hereinafter Opinion *France v Commission I* and *González Sánchez* .

Commission of the European Communities v French Republic, Case C-52/00." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62000CJ0052. Hereinafter Comission v France I.

Commission of the European Communities v Hellenic Republic, Case C-154/00." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62000CJ0154&qid=1659529345252. Hereinafter *Commission v Greece*

"María Victoria González Sánchez v. Medicina Asturiana, Case C-183/00." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3AC2002%2F180%2F08&qid=1659529978324. Hereinafter, *González Sánchez*.

"Federal republic of Germany v European Parliament and Council of the European Union, Case C-380/03." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62003CJ0380. Hereinafter, *Tobacco Advertising II*.

"Skov Æg v. Bilka Lavprisverehus A/S and Bilka Lavprisvarheus A/S v. Jette Mikkelsen and Michael Due Nielsen, Case C-402/03." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62003CJ0402&qid=1659528136269. Hereinafter *Skov Æg*

"Opinion of Advocate General Geelhoed Declan O'Byrne v Sanofi Pasteur MSD Ltd and Sanofi Pasteur SA." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A62004CC0127

Declan O'Byrne v. Sanofi Pasteur MSD Ltd and Sanofi Pasteur SA, Case, C-127/04." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62004CJ0127&qid=1659521717510. Hereinafter *O'Byrne*.

"Commission of the European Communities, Case, C- 177/04." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62004CJ0177 (hereinafter *Commission v France II*).

"The Queen, on the application of Vodafone Ltd and Others v Secretary of State for Business, Enterprise and Regulatory Reform, Case C-58/08." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62008CJ0058.

"Commission of the European Communities v Kingdom of Denmark, Case C-327/05." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62005CJ0327&qid=1659528164042. Hereinafter *Commission v Danemark*.

"Laval un Partneri Ltd v Svenska Byggnadsarbetareförbundet, Svenska Byggnadsarbetareförbundets avdelning, Byggettan and Svenska Elektrikerförbundet , Case C-341/05." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62005CJ0341.

"International Transport Workers' Federation and Finnish Seamen's Union v Viking Line ABP and OÜ Viking Line Eesti, Case C-438/05,"EUR-Lex." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62005CJ0438.

"Societé Moteurs Dalkia Somer v Dalkia France and Ace Europe, Case C-285/08." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62008CJ0285&qid=1659519214850

"Opinion of Advocate General Trstenjak, Aventis Pasteur SA v OB. Case C-358/08." EUR-Lex, Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62008CC0358.

"Aventis Pasteur SA v. OB, Case C-358/08." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62008CJ0358&qid=1659521893152. Hereinafter *Aventis Pasteur*.

"L'Oréal SA and Others v eBay International AG and Others, Case C-324/09." EUR-Lex. Accessed 31 January 2023.

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62009CJ0324.

"Centre hôspitalier universitaire de Besançon v Thomas Dutreux and Caisse Primaire d'assurance maladie du Jura, case, C-495/10." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62010CJ0495 (hereinafter *Centre hôspitalier Besançon*).

"Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, Cases C-293/12 and C-594/12." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293, hereinafter *Digital Rights Ireland*.

"Thomas Pringle v Government of Ireland and Others, Case C-370/12." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0370.

"Andreas Kainz v Panterwerke AG, Case C-45/13." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62013CA0045&qid=1659528811811. Hereinafter *Kainz v Panterwerke)*.

"Huawei Technologies Co. Ltd v ZTE Corp. and ZTE Deutschland GmbH,Case C-170/13." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62013CA0170. Hereinafter Huawei.

"František Ryneš v Úřad pro ochranu osobních údajů, Case C-212/13." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62013CJ0212, hereinafter Ryneš.

Opinion of Advocate General Szpunar, Novo Nordisk Pharma GmbH v S., Case, C-310/13," EUR-Lex. Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62013CC0310.

"Opinion of Advocate General Szpunar Novo Nordisk Pharma GmbH v S." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62013CC0310.

"Novo Nordisk Pharma GmbH v S., Case, C-310/13." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62013CA0310&qid=1659520416126 . Hereinafter *Novo Nordisk Pharma*.

Opinion of Advocate General Bot Boston Scientific Medizintechnik GmbH v AOK Sachsen-Anhalt – Die Gesundheitskasse and Betriebskrankenkasse RWE, Joined Cases C-503/13 and C-504/13." EUR-Lex, Accessed 31 January 2023.

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62013CC0503&qid=1659555918695.

"Boston Scientific Medezintechnik GmbH v AOK Sachsen-Anhalt(503) v Betriebskrankenkasse RWE (504), Cases C-503/13, C-504/13." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62013CJ0503&qid=1659519999217. Hereinafter *Boston Medezintechnik*).

"Peter Gauweiler and Others v Deutscher Bundestag, Case C-62/14." EUR-Lex**.** Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0062

"Patrick Breyer v Bundesrepublik Deutschland, Case C-582/14." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62014CJ0582.

"James Elliott Construction Limited v Irish Asphalt Limited, Case C-613/14." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62014CJ0613. Hereinafter, *James Elliott Construction*.

Opinion of Advocate General Bobek, N.W. and Others v Sanofi Pasteur MSD SNC and Others, Case C-621/15," EUR-Lex, Accessed 31 January 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62015CC0621

"Asociación Profesional Elite Taxi v Uber Systems Spain, SL, Case 434/15." EURlex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62015CJ0434.

N.W. and Others v. Sanofi Pasteur MSD SNC and Others, Case, C-621/15." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62015CJ0621&qid=1659519295161. Hereinafter *Sanofi Pasteur*.

Advocate General Eleanor Sharpston, delivered on 15 September 2016, Elisabeth Schmitt v. TÜV Rheinland LGA Products GmbH." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62015CC0219&qid=1659511812522

"Elisabeth Schmitt v. TÜV Rehinland LGA Prodcucts GmbH, Case C-219/15." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/GA/ALL/?uri=CELEX:62015CJ0219.

"Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV., Case C-40/17." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62017CJ0040.

"RB v. TÜV LGA Products GmbH and Allianz IARD S.A., Case C-518/18." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62018CJ0581.

"Google Alphabet v. Commission (Google Android), Case T-604/18." CURIA. Accessed 31 January 2023, https://curia.europa.eu/juris/liste.jsf?num=T-604/18

"VI v. KRONE- Verlag Gesellschaft mbH &Co KG, Case C-65/20." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62020CA0065&qid=1659528863098, hereinafter *Krone.*

"Hungary v European Parliament and Council of the European Union, Case C-156/21." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62021CJ0156.

"Republic of Poland v European Parliament and Council of the European Union, Case C-157/21." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62021CJ0157.

"Keskinäinen Vakuutusyhtiö Fennia v Koninklijke Philips N.V., Case C-264/21." EUR-Lex. Accessed 31 January 2023.

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62021CJ0264&qid=1659530426486.

Request for a preliminary ruling from the Oberster Gerichtshof (Austria) lodged on 12 May 2021 – UI v Österreichische Post AG

(Case C-300/21). Accessed 31 January 2023. https://curia.europa.eu/juris/document/document.jsf?text=&docid=244568&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=668819.

" Request for a preliminary ruling from the Cour de cassation (France) ldged on 18 November 2021-, Cafpi SA, Aviva Assurances SA v Enedis SA, Case C-691/21." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62021CN0691 .

"Opinion of Advocate General Campos Sánchez-Bordona delivered on 6 October 2022," EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1675182921469&uri=CELEX%3A62021CC0300.

" Cafpi SA and Aviva assurances SA v Enedis SA,Case C-691/21." EUR-Lex. Accessed 31 January 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62021CJ0691. Hereinfter *Cafpi Aviva v Enedis.*

5.2. Austria

GDPR HUB,OGH-6Ob35/21 x. Accessed 31 January 2023 . https://gdprhub.eu/index.php?title=OGH_-_6Ob35/21x_(request_for_preliminary_ruling_under_Article_267_TFEU)

5.3. France

Cour de Cassation, Première Chambre Civile, Arrêt n° 616 du 10 octobre 2018 (17-14.401), ECLI:FR:CCASS:2018:C100616.

5.4. Italy

Court of Cassation, 31 May 2003 n. 8827, Court of Cassation 31 May 2003 n. 8828

Court of Cassation Plenary Session (Sessioni Unite) 11 November 2008 n. 26972, n.26973, n. 26974 and n. 26975.

Court of Cassation Judgment n.7613, 15th April 2015.

Court of Cassation, Judgment n.16601, July 15th 2017.

Italian Court of Cassation, Third Section, n.7513/18, (President judge: G. Travaglino, Reporter judge: M. Rossetti). *Altalex*. Accessed 31 January 2023. https://www.altalex.com/massimario/cassazione-civile/2018/7513/risarcimento-del-danno-patrimoniale-e-non-patrimoniale-danni-morali-congiunta-attribuzione

Ordinanza Cassazione n.16402/2021. Accessed 31 January 2023.

https://i2.res.24o.it/pdf2010/Editrice/ILSOLE24ORE/QUOTIDIANI_VERTICALI/Online/_Oggetti_Embedded/Documenti/2021/06/11/16402.pdf.

5.5. UK

Winterbottom v. Wright, Exchequer of Pleas, 1842, 10 M. & W. 109, 152 Eng. Rep.402.

"Lloyd (Respondent) v Google LLC (Appellant), UKSC 2019/0213." *The Supreme Court* (official website). Accessed 31 January 2023. https://www.supremecourt.uk/cases/docs/uksc-2019-0213-judgment.pdf.

5.6. US

Stuart v. Wilkins, 1 Doug 18, 99 Eng. Rep. 15 (1778).

Lawrence v. Fox, N.Y. 268.

Burr v. Beers, 24 N.Y. 178.

Baxter v. Ford Motor Co. Supreme Court of Washington, 1932. 168 Wash. 456, 12 P.2d 409.

Escola v Coca Cola, Supreme Court of California, July 5, 1944

Henningsen v Bloomfield Motors Inc, Supreme Court of New Jersey, May 6 1960

Greenman v. Yuba Power Products, Inc. Supreme Court of California, 1963, 59 Cal.2d 57, 377 P. 2d 897, 27 Cal. Rptr 697.

Caterpillar Tractor v. Beck, 593 P.2d 871, 880, Alaska 1979.

Prentis v. Yale Mfg. Co., Supreme Court of Michigan, 1984. 421 Mich. 670, 365 N.W. 2d 176.

O'Brien v Muskin Corp. Supreme Court of New Jersey, 1983. 94 N.J. 169, 463 A 2d 298.

Rix v. General Motors Corp., Supreme Court of Montana, 1986. 222 Mont. 318,723 P.2d 195

Anderson v. Owens- Corning Fiberglas Corp. Supreme Court of California, 1991. 53 Cal3d, 810 P.2d 549, 281 Cal. Rptr.528

Hill v. Natl Collegiate Athletic Ass'n, 7 Cal 4th 1 (Cal.1994), 26 Cal. Rptr. 2d 834 865 P 2d 633.

Medtronic v. Lohr, 518 U.S. 470 (1996), hereinafter *Lohr*.

Briehl v. General Motors Corp.,172 F.3d 623 (8th Cir. 1999),

Buckman v. Plaintiffs' Legal Comm., 531 U.S. 341(2001),, hereinafter *Buckman*.

Riegel v. Medtronic, 552 U.S. 312 (2008), hereinafter *Riegel.*

O'Neil v. Simplicity, Inc., 574 F.3d 501 (8th Cir. 2009)

Birdsong v. Apple Inc., 590 F.3d 955 (9th Cir. 2009).

In Re Toyota Motr Corp. Unintended Acceleration Marketing Sales Practices and Products Liability Litigation, 754 F. Supp. 2nd 1145 (C.D. Cal. 2010)

In re I-phone Application Litigation No 11-MD-02250-LHK 2011 WL 4403963 *5 (N.D. Cal. Sept. 20 2011).

Reilly v. Ceridian Corp., 664 F.3d 38, 43 (3rd Cir. 2011).

PILVA, Inc. V. Mensing, 564 US 604, 618-19 2011

In re Zurn Pex Plumbing Products Liability Lit. 644 F.3d 604 (8th Cir. 2011)

Thunander v. Uponor, Inc., 887 F. Supp. 2d 850 (D. Minn. 2012),

George v. Uponor Corp., ___ F. Supp. 2d ___, 2013 WL 6801219 (D. Minn. Dec. 23, 2013)

Hinojos v. Kohl's Corp, 718 F.3d 1098 (9th Cir.2013).

"Clapper v. Amnesty International USA, 838 F. 3d 118,(2013)" Legal Information Institute. Accessed 31 January 2023. https://www.law.cornell.edu/supremecourt/text/11-1025.

U.S. Hotel and Resort Management, Inc., et al.,v. Onity, Inc. United States District Court-District of Minnesota, Civil No. 13-1499 (SRN/FLN), 2014. Accessed 31 January 2023. https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1818&context=historical.

In re MyFord Touch Consumer, 46 F.supp 3rd 945 (2014). Herinafter *MyFordTouch.*

Accord Galaria v. Nationwide Mut. Ins. Co. F. Supp. 2d, 2014 WL 689703, *5, *7 (S.D. Ohio Feb. 10, 2014).

U.S. Hotel and Resort Management, Inc., et al.,v. Onity, Inc. United States District Court-District of Minnesota, Civil No. 13-1499 (SRN/FLN), 2014.

In re Sony Gaming Newtorks & Customer Data Security Breach Litigation, 996 F. Supp. 2nd 942 (S.D. Cal 2014).

Cahen v. Toyota Motor Corp., 147 F. Supp. 3d955 (N.D. Cal. 2015). Accessed 31 January 2023. https://casetext.com/case/cahen-v-toyota-motor-corp-3. Hereinafter *Cahen I.*

Archer-Hayes v. ToyTalk, Inc., No. BC603467, 2015 WL 8304161 (Cal. Super. Dec. 7, 2015)

Riva v. Pepsico, 82 F. Supp. 3d 1045, 1052 (N.D. Cal 2015).

Spokeo, INC. v. Robins, 136 S.Ct.1540 (2016), hereinafter, *Spokeo*

Cahen et al v. Toyota Motor Corporation, Toyota Motor Sales, U.S.A., INC., and General Motors LLC, Case 16-15496 (2016). Accessed 31 January 2022. https://casetext.com/case/cahen-v-toyota-motor-corp-2.

United States Distrct Court For the Northern District of Illinois Eastern Division *IN RE VTECH DATA BREACH LITIGATION No 15 CV 10889, No15 CV 10891, No15 CV 11620, and No15 CV 11885*,(2016)" Casetext, Accessed 31 January 2023, https://casetext.com/case/in-re-vtech-data-breach-litig-1.

Freed v. St. Jude Med., Inc., Civil Action No. 17-1128-CJB, 2019

WL 5102643 (D. Del. Oct. 11, 2019)

Mellott v. St. Jude Med., LLC, Civil Action No. 19- 1779-CJB (D. Del. Nov. 16, 2020) (D.I. 45 at 7-8, 9-14),

Guinn v St Jude Medical LLC 20-71-CJB, D.I. 50 (*Guinn I*) 2020

Guinn v. St Jude Medical LLC, LLC 20-71-CJB, D.I. 77 (*Guinn II*) 2021,

Colleen Ross v St Jude Medical LLC, N. 20-971-CJB (Ross) 2021.

5.6.1. FTC orders and decisions

"In the Matter of TRENDNet, 2014." Federal Trade Commission. Accessed 31 January 2023. https://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf.

Hereinafter *TRENDnet* Complaint.

"In the Matter of TRENDNet ,2014." Federal Trade Commission. Accessed 31 January 2023. https://www.ftc.gov/system/files/documents/cases/140207trendnetdo.pdf.

.Hereinafter *TRENDnet* Decision and Order

"In the Matter Vizio, 2017." Federal Trade Commission. Accessed 31 January 2023. https://www.ftc.gov/system/files/documents/cases/170206_vizio_stipulated_proposed_order.pdf.

Hereinafter, *Vizio* Decision and Order.

"VTech Electronics Limited, 2018." Federal Trade Commission. Accessed 31 January 2023. https://www.ftc.gov/system/files/documents/cases/vtech_file_stamped_complaint_w_exs_1-8-18.pdf. Hereinafter VTech Complaint.

"VTech Electronics Limited, 2018." Federal Trade Commission. Accessed 31 January 2023.

https://www.ftc.gov/system/files/documents/cases/vtech_file_stamped_stip_order_1-8-18.pdf. Hereinafter,

VTech Stipulated Order.

D-Link Complaint, Redacted Version, 2019." Federal Trade Commission, Accessed 31 January 2023, https://www.ftc.gov/system/files/documents/cases/170105_d-link_complaint_and_exhibits.pdf, hereinafter D-Link complaint.

"In matter D-link, 2019." Federal Trade Commission, Accessed 31 January 2023, https://www.ftc.gov/system/files/documents/cases/dlink_proposed_order_and_judgment_7-2-19.pdf. Hereinafter, D-Link Decision and Order.

"In the Matter of Tapplock, Inc., 2020." Federal Trade Commission, Accessed 31 January 2023, https://www.ftc.gov/system/files/documents/cases/1923011c4718tapplockcomplaint.pdf, hereinafter Tapplock complaint.

"In the Matter of Tapplock, Inc., 2020." Federal Trade Commission, Accessed 31 January 2023, https://www.ftc.gov/system/files/documents/cases/1923011c4718tapplockorder.pdf Hereinafter Tapplock Decision and Order.

Personal acknowledgments

There are so many people to thank for this thesis that I am afraid this page could turn out to be an essay, but I will try to be brief.

I would like to thank Professor Monica Palmirani, from Alma Mater Studiorum University of Bologna, for her unwavering support throughout this PhD which took place through a pandemic and a war. Without her vision, this Marie Skłodowska Curie grant would have been very different.

I sincerely thank my supervisor, Professor Mindaugas Kiškis, from Mykolas Romeris University, for his continuous availability and support throughout my PhD.

I must thank Professor Giovanni Sartor, my supervisor from Alma Mater Studiorum University of Bologna, for the inputs given throughout my PhD.

I would like to thank Professor Michele Graziadei from the University of Turin for his kindness, availability and the many things learned. But, most importantly, I am grateful that he made me understand the mind-set with which research is done: to never be afraid to look for the best you can get from yourself while knowing at the same time that a finished article, essay or thesis is just a starting point for many more interesting research paths.

I would sincerely thank Professor Dovilė Sagatienė from Mykolas Romeris University for being a mentor and for showing me that research has also to come out of articles and books and to become an occasion of discussion and debate with many other minds, different and alike.

I must thank Professor Carles Górriz López, from Universitat Autònoma de Barcelona for his kindness and support through the draft of the deliverable within this PhD project.

Most importantly, I would like to thank my family in Mirandola, Stockholm and Vilnius, for being a safe harbour to which I can always set sail. Words cannot precisely express the amount of love and gratitude I have towards you, and I can just hope I can be worth of you all. A huge thank you and a hug to all my friends scattered around Europe and beyond. You know who you are. Thank you for accepting me and for always being there for me, but especially when in need of help or comfort.

Last, but definitely not least, Aurimas, my boyfriend, is the person without whom this thesis and many other things would not have been possible and that is why this thesis is dedicated to him.