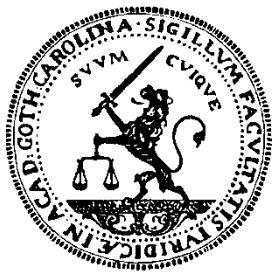

FACULTY OF LAW
Lund University

Felicia Johansson

Can things be defective products?

An analysis of the Product Liability Directive applied to IoT

JURM02 Graduate Thesis

Graduate Thesis, Master of Laws program
30 higher education credits

Supervisor: Marja-Liisa Öberg

Semester of graduation: Period 1 Spring semester 2021

Table of Contents

Summary

The number of products equipped with sensor and network capabilities has risen in recent years and continues to increase. These products, part of the Internet of Things (IoT), bring about new ways for products intended for private use to malfunction and cause personal injury and property damage. In the EU, the Product Liability Directive (PLD) regulates producers' strict liability for damage to other products than the one causing the damage and for harm to persons. The damage must be ascribable to a "product" that is "defective" in the meaning of the PLD. For some types of defect, the producer can invoke liability exemptions. However, the PLD was adopted prior the widespread use of the internet and long before digital technologies become incorporated into billions of consumer products. The concepts of product and defect and the available liability exemptions, therefore, do not explicitly regulate the unique characteristics of IoT.

The purpose of this thesis is to critically examine if the concepts of product and defect, as they are understood within the PLD, are flexible enough to encompass damages caused by IoT products. This involves addressing the characteristics of IoT products, analysing case law, evaluating the European Commission's soft law instruments on emerging digital technologies and comparing the PLD to similar consumer protection regulation.

The thesis finds that not all digital elements of IoT fall within the scope of the Directive. The deciding factor for IoT products to be regarded as products in the meaning of the PLD is that they are not intangible services. While software that comes pre-installed in IoT products are components covered by the PLD, the same cannot with certainty be said about, e.g., software updates or interconnected cloud systems. Both the distinction between services and products and principles such as functional equivalence are examined to reach this conclusion.

Moreover, the thesis addresses that the static concept of defect makes the PLD ill-equipped to regulate liability for IoT products. The possibility to change products through updates – and, when technology advances, self-learning software – after the product reaches the consumer, renders the provisions of the PLD archaic. The issue mainly lies in that the assessment of defect is firmly anchored in the moment when the product was "put into circulation".

The thesis presents that these shortcomings, which leave liability for IoT products regulated partially differently than other products, could be solved through drastic alterations to the PLD. Changes to the current regime would require careful consideration of the variety of products on the market today and in the future, as well as to the interests of all parties, to fulfil the aim set out in the PLD of complete harmonisation of strict liability for all products.

Sammanfattning

På senare år har mängden produkter utrustade med sensorer och nätverksfunktioner ökat och fortsätter att öka. Dessa produkter, del av Sakernas Internet (IoT), möjliggör nya sätt för produkter avsedda för privat bruk att gå sönder och orsaka person- och sakskada. På EU nivå reglerar produktansvarsdirektivet (PLD) tillverkarens strikta ansvar för skador på andra produkter än den felande produkten samt personskador. Skadan måste kunna tillskrivas en ”produkt” som har en ”säkerhetsbrist”. För vissa typer av fel kan tillverkaren åberopa undantag från ansvar. PLD antogs före det att internetanvändning blev utbrett och långt före digital teknik inkorporerades i miljarder konsumentprodukter. Begreppen produkt och säkerhetsbrist, samt de tillgängliga grunderna för ansvarsfrihet, reglerar därför inte uttryckligen de unika egenskaperna i IoT.

Syftet med denna uppsats är att kritisk undersöka om begreppen produkt och säkerhetsbrist, så som de tolkas i PLD, är tillräckligt flexibla för att reglera skador orsakade av IoT-produkter. De unika egenskaperna hos IoT-produkter, relevant rättspraxis, EU-kommissionens icke-bindande rättsakter om ny digital teknik samt närliggande konsumentskyddslagstiftning analyseras för att uppfylla syftet.

Uppsatsen finner att inte samtliga digitala aspekter av IoT faller inom direktivets tillämpningsområde. Den avgörande faktorn i detta avseende är om delar av IoT-produkter ska betraktas som produkter eller som immateriella tjänster. Medan förinstallerad mjukvara i IoT-produkter utgör en komponent som täcks av PLD, kan inte detsamma med säkerhet sägas om exempelvis mjukvaruuppdateringar eller molnsystem som är sammankopplade med produkten. Både skillnaden mellan tjänster och produkter samt principer så som funktionell ekvivalens undersöks för att nå denna slutsats.

Därutöver behandlar uppsatsen att det statiska begreppet defekt medför att PLD är dåligt utrustad för att regla produktansvar för IoT-produkter. Möjligheten att kontinuerligt förändra produkter genom uppdateringar – samt, till följd av tekniska framsteg, självlärande programvara – efter att produkten har nått konsumenten innebär att PLD kan uppfattas som ålderdomlig. Problemet är huvudsakligen en följd av att bedömningen av om en säkerhetsbrist föreligger eller inte är förankrat i den tidpunkt då produkten ”satts i omlopp”.

Uppsatsen presenterar även att dessa brister, som orsakar att ansvar för IoT-produkter delvis regleras annorlunda än andra produkter, skulle kunna lösas genom drastiska förändringar i PLD. Ändringar av det gällande produktansvarssystemet skulle kräva noggranna överväganden angående den breda variationen av produkter som finns på marknaden, liksom parternas intressen, för att uppfylla det i PLD uppsatta målet om fullständig harmonisering av strikt ansvar för samtliga produkter.

Abbreviations

AI	Artificial Intelligence
AG	Advocate General
CJEU	Court of Justice of the European Union
IoT	Internet of Things
OTA	Over-the-air
PLD	Product Liability Directive
RED	Radio Equipment Directive
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union

Preface

Med detta examensarbetearbete har min tid som juriststudent nått sitt slut. Precis som alla andra som har tagit sig igenom nio terminer på juristprogrammet har jag många att tacka för dessa givande och utvecklande år.

Jag vill börja med att tacka min handledare Marja-Liisa Öberg för allt stöd under uppsatsskrivandet och för att du har stått ut med mina mejl på konstiga tider. Tack till mina vänner som har förgyllt studietiden. Tack till Maria, för att du alltid finns där. Stort tack till pappa för de otaliga timmar du genom åren har lagt på att lusläsa mina uppsatser och för de ovärderliga råd som har gjort att texterna gått från utkast till slutprodukt. Inte minst gällande detta examensarbete.

Slutligen vill jag tacka Lund, Juridiska Föreningen, Fadderprogrammet och hela studentlivet för alla minnen.

Lund, 25 maj 2021
Felicia Johansson

1 Introduction

1.1 Background

The Internet of Things (IoT) is increasingly influencing people's everyday lives. Similar to how people can keep in contact over the internet, IoT makes possible continuous communication between *things*. That traditionally unconnected items can communicate with one another is no longer a futuristic utopia. Billions of items that fall within the concept of IoT are already on the market and there are signs that the purchase rate of smart devices is increasing during ongoing pandemic.[1] With technological progress, the trend towards all things ingrained with IoT will advance even further.

IoT brings with it a greater interconnectedness between items part of the material world and items of the digital world. Without sensors, cloud services, internet connection and software, smart devices would not function properly. However, while the material aspects of products on the market often stay unchanged throughout a product's lifetime, the software and data that are part of smart devices is much more dynamic. Updates can alter the functionalities of the products or create security risks and self-learning capabilities can be part of the digital makeup of smart devices. Furthermore, proneness to cyber security attacks is a reported weakness of smart devices. The technological characteristics of smart devices, therefore, lead to new types of product malfunctions and damages.

---

[1] Lueth K, 'State Of The Iot 2020: 12 Billion Iot Connections, Surpassing Non-Iot For The First Time' (*IoT Analytics*, 2021) https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/ accessed 18 May 2021; Parks Associates, 'Parks Associates: 33% Of Smart Home Device Owners Report Increased Usage During The COVID-19 Pandemic' (*Prnewswire.com*, 2021) https://www.prnewswire.com/news-releases/parks-associates-33-of-smart-home-device-owners-report-increased-usage-during-the-covid-19-pandemic-301197501.html accessed 20 May 2021.

In the EU, strict extra-contractual liability for damages caused by defective products is governed by the Product Liability Directive (PLD).[2] Several concepts are key in determining if an injured person can claim liability from a product producer under the Directive, including, among others, the notions of "product" and "defect". Even if the necessary conditions are fulfilled, exemptions can limit the producer's liability.

These concepts and provisions, along with the rest of the law, have remained mostly unchanged since the adoption of the PLD in 1985. The PLD is technological neutral and has been praised for being adaptable to developments on the market. Yet, the rapid move towards complex digital products was not foreseen in the early 1980s. In the past few years, the Commission has highlighted that there exist uncertainties on how the concepts and provisions of the PLD should be interpreted when applied to emerging digital technologies. These uncertainties make it unclear to what degree the PLD is applicable to the unique characteristics of products that incorporate emerging digital technologies.

More often than not, however, the Commission's documents do not differentiate between different types of products reliant on different emerging digital technologies. The concepts of IoT, artificial intelligence, advanced robotics, autonomous systems, 3D printing, apps, and non-embedded software are often bundled together into the umbrella term "emerging digital technologies" without much care about the wide array of applications these technologies can have. Moreover, in dept analysis of what exact difficulties the technologies pose for the application of the PLD is seldom provided.

[2] 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 [1985] OJ L 210/29.

1.2 Purpose and research question

The overarching purpose of the thesis is to examine to what extent the PLD applies to IoT objects.[3] Specifically, the thesis seeks to answer the question of whether the characteristics of IoT objects are at conflict with the notions of product and defect.

In view of the purpose of the thesis, the following research questions will be examined:

- What is IoT?
- How does the PLD define the concepts of "defect" and "product"?
- Are there aspects of IoT objects that do not fall within the legal definitions of product and defect?

1.3 Methodology and material

A doctrinal legal methodology will be applied in the thesis. The doctrinal legal methodology uses accepted sources of law to interpret and describe law.[4] Both *de lege lata* and argumentations *de lege ferenda* fall within the do methodology. In other words, the doctrinal legal methodology is concerned with descriptions and interpretations of what current legislation is as well as what it ought to be. However, more liberal argumentations on how legislation ought to be applied or formulated to achieve, for example, ethically correct

[3] Throughout this thesis, "things" that use IoT techonology will be called objects. An alternative would be to refer to them as products, which is the terminology often used on the market, but this could create confusion between "product" in the general sense of the word and "product" within the meaning of the PLD.

[4] Nääv M and Zamboni M, Juridisk metodlära (2nd edn., Student-litteratur, 2018), p. 21.

results or results motivated by specific judicial policies is not covered by the dogmatic legal methodology.[5]

As the thesis has an EU perspective, the EU's sources of law and methods of interpretation will be of relevance throughout the thesis. Like many other legal systems, the EU has a hierarchical system of sources of law.[6] The highest-ranking level consist of EU primary law, made up of the TEU, TFEU, the Charter and the general principles of law.[7] Below primary law is secondary law. The upper two sources of law are complemented by other sources of law, such as case law from the Court of Justice (CJEU).[8]

The foundation of this thesis is secondary EU law. Secondary law is made up of binding acts in the shape of regulations, directives, decisions as well as non-binding acts, such as recommendations and opinions.[9] There is no inherent hierarchy between the different binding, legislative acts of secondary law.[10] The acts do, however, differ. The focus of this thesis is the PLD, why an underlying understanding of directives is especially important. Contrary to regulations, directives are not directly applicable in Member States.[11] Directives must be transposed into Member States' national legislation in a way that is in conformity with the provisions and objectives of the directive.[12] In

---

[5] Sandgren C, "*Rättsvetenskap för uppsatsförfattare: Ämne, material, metod och argumentation*" (4th Edition, Nordstedts Juridik, 2018), p. 48ff.

[6] Riesenhuber K, *European Legal Methodology* (Intersentia 2017), p. 119f.

[7] Consolidated Version of the Treaty on European Union (TEU) [2008] OJ C115/13, Article 6; Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union (TFEU) [2016] OJ C202/1, Article1(2); Hettne J, and Otken Eriksson I, *EU-Rättslig Metod: Teori Och Genomslag I Svensk Rättstillämpning* (2nd edn, Nordstedts Juridik 2011), p. 44.

[8] Riesenhuber (2017), p. 120.

[9] TFEU Article 288.

[10] Hettne and Otken Eriksson (2011), p. 45f.

[11] TFEU, Article 288.

[12] TFEU, Article 288; see also TEU, Article 4 para 3 on the general principle of union loyalty; Riesenhuber (2017), p. 320f.

other words, no provisions in a Member State's national legislation should be at conflict with the PLD.[13] The obligation to interpret national legislation in conformity with a directive also extends to interpretations by national courts.[14] Thus, despite directives not being the acts persons turn to in order to claim rights or responsibilities – as they rely on national implementations – the wording and purpose of directives continue to be crucial *de lege lata* and *de lege ferenda* even after transposition into national law.

To bring clarity to what changes a future revision of the PLD, or an interpretation by the Court, could result in, the area of product liability is briefly compared to secondary EU legislation on product safety and sale of goods. Product safety is a legal area closely tied to that of product liability and a comparison is therefore suitable. Regulation on sales of goods to consumers is appropriate as it regulates conformity of sales contract and contractual (rather than non-contractual) liability. The secondary legislations chosen for the analogy regulate digital technologies. When carrying out comparisons between legal areas, one must keep in mind that the political and social factors present at the time of the adoption of the newer safety legislation differ from the situation present when the PLD was adopted.[15]

Binding secondary legislation, as well as primary legislation, begin with preambles. The recitals therein present the legislator's intentions for the act.[16] In this thesis, recitals are referred to where they deepen the understanding of the legislator's intentions. Preambles do not have autonomous binding legal force

[13] Hettne and Otken Eriksson (2011), p. 179.

[14] Case C-14/83, *Sabine von Colson and Elisabeth Kamann v Land Nordrhein-Westfalen* EU:C:1984:37, paras 26 and 28.

[15] Alter K, Dehousse R, and Vanberg G, 'Law, Political Science and EU Legal Studies' (2002) 3 European Union Politics, p. 116f.

[16] Riesenhuber (2017), p. 248.

and cannot be relied on to interpret an act in a way that deviates from the wording of its provisions, but are an interpretive aid for the CJEU.[17]

Non-binding secondary legislation is commonly referred to as *soft law* and is used extensively by the EU's institutions.[18] There is no exhaustive list of what types of EU instruments constitute soft law, but it has been described as consisting of "rules of conduct which, in principle, have no legally binding force but which nevertheless may have practical effects."[19] The practical effects stem from the change in behaviour of Member States or EU institutions that the instrument may invoke.[20] Limited legal effects have also been acknowledged, despite soft law not being legally binding.[21] Throughout this thesis, non-binding secondary legislation on product liability and product safety, such as working documents, reports and communications are extensively consulted. They give insight into the Commission's interpretation of the PLD, though seldom providing in-depth commentary. The sources are used both as starting points when uncertainties regarding the PLD are discussed and as evidence for how the notions of the PLD are likely to be understood by the court and Member States.

---

[17] Case C-136/04 *Deutsches Milch-Kontor GmbH v Hauptzollamt Hamburg-Jonas* EU:C:2005:716, para 32; Riesenhuber (Intersentia 2017), p. 248; See also for example Case C-495/10 *Centre hospitalier universitaire de Besançon v Thomas Dutrueux and Caisse primaire d'assurance maladie du Jura* EU:C:2011:706, para 24.

[18] Hettne and Otken Eriksson (2011), p. 46.

[19] Snyder F, 'The Effectiveness of European Community Law: Institutions, Processes, Tools and Techniques' (1993) 56 The Modern Law Review, p. 32; see also Stefan O A et al., 'EU Soft Law in The EU Legal Order: A Literature Review' [2019] SSRN Electronic Journal, p. 10.

[20] Stefan et al. (2019), p. 22.

[21] Case C-322/88 *Salvatore Grimaldi v Fonds des maladies professionnelles* EU:C:1989:646, para 18; see also Snyder, F., 'Interinstitutional Agreements: Forms and Constitutional Limitations' (1994) European University Institute, p, 14 and 16-17.

Another central source of law within the EU is case law of the CJEU.[22] Only a few cases concerning the PLD have been brought to CJEU. All cases that have a bearing on the interpretation of the relevant concepts and provision are examined and compared to the situations that may arise because of defects in IoT. Rulings that define the scope and meaning of EU law in general are also presented. The Court is not formally bound by its earlier decisions.[23] Changes in for example society can lead the Court to change direction in later case law.[24] The detailed opinion of the Advocate General (AG) is referred to in the examination where it furthers the understanding of a ruling. The AG's opinion plays an advisory role to the CJEU.[25] It is only where the Court refers to or has been clearly influenced by the AG's opinion that it holds value as a legal source.[26]

Finally, the essay will make use of legal doctrine, particularly for examining how the PLD relates to the characteristics of IoT.

1.4 Delimitations

This thesis aims to analyse the EU's harmonised product liability regime, established through the PLD, as applied to damages caused by IoT used by consumers for private purposes. Non-harmonised legislation, such as liability for specific people or fault-based liability, is not covered by the thesis. Much of the legislation and legal issues concerning autonomous vehicles – a type of IoT – is therefore not detailed in the thesis.

This short thesis cannot give a holistic approach to the entirety of the PLD. The focus lies only on the concepts of product and defect within the meaning

[22] Hettne and Otken Eriksson (2011), p. 49f.

[23] Hettne and Otken Eriksson (2011), p. 51 and 60.

[24] Hettne and Otken Eriksson (2011), p. 51 and 60.

[25] Hettne and Otken Eriksson (2011), p. 116f.

[26] Hettne and Otken Eriksson (2011), p. 117.

of the PLD. Within this also falls an examinations of liability exemptions, due to the close bond with the notion of defect. Other aspects of the PLD will not be addressed. For instance, the topics of burden of proof and of who is the most suitable to hold liable in cases where the PLD applies will not be covered. This is not to say that liability allocation or burden of proof are irrelevant when discussing IoT. On the contrary, one can except to see changes in how the EU approaches these topics when damage has been caused by emerging digital technologies. The notion of "damage" and the ongoing debate of whether it should be expanded to include stolen personal data, or if the GDPR is better suited to address such cyber-attacks, is another topic that is not covered in this essay.

Although industrial IoT is a large field, this thesis only focuses on IoT being used for private purposes. Subjects such as the protection against cyber security risks for essential infrastructure, regulated by the NIS-directive, will therefore not be discussed.

1.5 Previous research

There is an apparent lack of research on the PLD focused solely on IoT. More has been written about emerging digital technologies in general, much of which gives an overview of the multitude of liability issues that the technologies have brought about without going into detail. However, the possibilities and legal risks with self-learning AI has gained abundant attention among scholars. Autonomous cars are often presented as the principal example when legal implications of sophisticated self-learning AI are evaluated.

A great body of work can be found about software. Software has interested legal scholars since at least the 1990s. A drawback of software gaining most attention among legal scholars in the decades prior to internet usage becoming widespread, is that software updates have not been addressed to the same extent as, for example, software supplied on CD's.

This thesis adds to the research by going in depth on a limited number of areas of the PLD in regard to IoT. In contrast to a lot of research on emerging digital technologies, this thesis pursues to sway away from dystopian predictions of self-learning AI as an omnipresent threat to the current liability regime.

1.6 Outline

The second chapter addresses the technical aspects of IoT and outlines what differentiates IoT objects from products without digital elements. Some of the risks these characteristics present are also outlined. The third chapter examines the PLD on both a general level and, regarding the notions of product and defect as well as the later defect defence and development risk defence, in detail. This is necessary for the in-depth analysis carried out in the fourth chapter. In the fourth chapter, the provisions addressed in the third chapter are evaluated against the characteristics of IoT. A conclusion and general discussion of the earlier chapters follows in the fifth chapter.

2 What is the IoT?

2.1 Definition and technical development

The IoT refers to everyday objects – "things" – that are interconnected with other objects through the internet. Sensors, software, electronics and network connectivity make up the digital aspects of the objects, which are embedded into the material parts of the objects.[27] The purpose of the intricate but seamless intertwining between material and digital parts is to optimise efficiency and enhance the user experience.[28]

In the consumer setting, IoT objects include many of the products that are labelled as "smart", i.e., to some degree automated. Smart fitness watches and smart baby monitors are but two examples. One popular category of consumer IoT is smart homes. Smart homes are ecosystems made up of interconnected devices and appliances, such as thermostats, lighting fixtures, kitchen appliances and security devices.[29]

A complex and constantly ongoing chain of events create the data driven infrastructure of IoT objects. Real time data is collected by sensors, that are either integrated into the device or form part of an external source.[30] The gathered data can be transferred over the internet, without human interaction, between interconnected objects. The data is most often processed, i.e., analysed,

---

[27] Tschider instead categorise IoT devices into three groups: physical, smart and connectivity components, see Tschider C, 'Regulating the Internet of Things: Discrimination, Privacy, And Cybersecurity In The Artificial Intelligence Age' [2018] SSRN Electronic Journal, p. 92.

[28] Tschider (2018), p. 93; DeNardis L, *The Internet in Everything: Freedom And Security In A World With No Off Switch* (Yale University Press 2020), p. 29f.

[29] DeNardis (2018), p. 26.

[30] Barbero M, et al., 'Study on Emerging Issues of Data Ownership, Interoperability, (Re-)Usability and Access to Data, And Liability' (European Union 2018) May 2021, p. 103.

in and mediated through a cloud system.[31] The system's cloud computing takes place in central servers and is thus not materially part of any of the IoT objects.[32] As a compliment to cloud computing, the processing step in certain IoT ecosystems can partially be carried out in gateway devices or "at the edge", i.e., closer to the material location of IoT objects. This is done to reduce the large amount of continuous data sent to the cloud over the internet.[33] Still, the IoT infrastructure is dependent upon cloud services' big data computing and storage.[34] After the almost instant processing, the data can automatically activate actuators to set off changes in the material world.[35] The objects can also be remotely monitored and controlled by users through smartphone apps or voice controlled personal assistants connected to the IoT object.[36] Ongoing monitoring of IoT objects can likewise be carried out by the producer.[37]

The proper functioning of the objects also relies on software. Software is the information that operates an object with digital elements.[38] While software does come embedded into the objects, many IoT objects can also be updated remotely through so called over-the-air updates (OTA).[39] OTA updates can be downloaded automatically or require the user to manually accept the

---

[31] Noto La Diega G, 'Clouds of Things: Data Protection and Consumer Law at the Intersection of Cloud Computing and the Internet of Things in the United Kingdom' (2016) 9 Journal of Law & Economic Regulation, p. 75.

[32] Adi E et al., 'Machine Learning and Data Analytics for The Iot' (2020) 32 Neural Computing and Applications, p. 6f.

[33] Adi et al. (2020), p. 7

[34] Tschider (2018), p. 91f.

[35] Barbero et al. (2018), p. 104.

[36] Tschider (2018) p. 91 and 120.

[37] Tschider (2018), p. 95f.

[38] Commission, 'Evaluation of Council Directive 85/374/EEC on the approximation of laws, regulations and administrative provisions of the Member States concerning liability for defective products - Final report' (2018c), p. 174.

[39] Bauwens J et al., 'Over-The-Air Software Updates In The Internet Of Things: An Overview Of Key Principles' (2020) 58 IEEE Communications Magazine, p. 1.

download. Through the use of updates, producers are changing the objects after they have been sold to consumers, often as a result of a "ship now, patch later" approach to programming.[40]

2.2 Risks with IoT

IoT objects come with unique risks. Many of which can be attributed to the fact that the IoT market is young and that actors involved consequently do not have the necessarily background in building secure software that interacts with the world.[41] Cyber security weaknesses is a well reported issue of IoT.[42] Not only can unauthorised access lead to economic loss or personal data being stolen; an attacker could gain access to a connected material device and cause harm to both property and people.[43] As devices on the same network can be interconnected, a weak link in any of the devices could act as an entry point for a cyber-attack on any of the connected devices.[44]

Additionally, faulty software could potentially lead to material damage even without poorly integrated security features, for example by misreading data

---

[40] Dean B, 'An Exploration of Strict Products Liability and The Internet of Things' (2018) SSRN Electronic Journal, p. 3 footnote 3.

[41] Knox Everette W, 'Security Vulnerabilities, The Current State of Consumer Protection Law, & How IOT Might Change It' (*Youtube*, 2016) https://www.youtube.com/watch?v=EFGcZwjw9Q4 accessed 18 May 2021.

[42] See for example Hessel S and Rebmann A, 'Regulation of Internet-of-Things cybersecurity in Europe and Germany as exemplified by devices for children' (2020) International Cyber-security Law Review.

[43] Lucian Constantin B, 'Hackers found 47 new vulnerabilities in 23 IoT devices at DEF CON' (*Computerworld*, 2016) https://www.computerworld.com/Article/3118762/hackers-found-47-new-vulnerabilities-in-23-iot-devices-at-def-con.html accessed 18 May 2021; Dean (2018), p. 1.

[44] Hay Newman L, 'An Elaborate Hack Shows How Much Damage Iot Bugs Can Do' (*Wired*, 2021) https://www.wired.com/story/elaborate-hack-shows-damage-iot-bugs-can-do/ accessed 18 May 2021.

or through malfunction.[45] The faulty software can be introduced either when the product is sold or through subsequent software updates.[46] Another weakness is the reliability on real time data and constant network connection for IoT objects to function. If there is a disturbance in the amount or accuracy of data that is gathered or transferred between devices, or in case of a network failure, a ripple effect of malfunctions could occur.[47] For example, a smart door-lock that should automatically open when a fire breaks out fails to receive the fire alert from the cloud and, simultaneously, fails to connect to the trapped owner's smartphone for manual unlock.[48] The intertwining of the digital and material world can thus cause damages that are not attributable to the tangible parts of objects.

2.3 Understanding AI

Artificial Intelligence (AI) is a concept that is often bundled together with IoT when new technologies are discussed by the EU commission.[49] Some IoT is reliant upon AI, but AI is not one thing. Treating it as such paints a false picture of the risks and opportunities that come with AI.

There does not exist one unifying definition of AI. In fact, defining AI is a moving target. Once a technological process regarded as AI has been achieved, it is often no longer seen as intelligent.[50] Despite this, it is generally

---

[45] Zoeller F E et al., 'More Soft Landings for Software: Liability for Defects in an Industry That Has Come of Age' (2005) 21 Santa Clara High Technology Law Journal, p. 746 and 769.

[46] Commission, Commission Staff Working Document, 'Liability for emerging digital technologies', SWD (2018) 137 final (2018b), p. 10.

[47] Commission, Commission Staff Working Document (2018b), p. 10.

[48] European Law Institute, 'Guiding Principles for Updating The Product Liability Directive For The Digital Age' (2021), p. 8.

[49] See especially Commission, 'Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics' COM (2020) 64.

[50] Turner J, *Robot Rules: Regulating Artificial Intelligence* (Palgrave Macmillan 2019) p. 8.

accepted that AI refers to systems that processes large amount of data (big data) and, based on that processing, make autonomous decisions to achieve specific goals.[51] There are AI systems that can adjust and improve over time by analysing its previous actions to find patterns.[52] The identified patterns can also be used to predict future outcomes. Such systems thus possess the power of self-learning.[53] The data that leads the AI to optimise over time can, e.g., originate from sensory input from the environment.

Some level of autonomy is incorporated into IoT infrastructure. The real-time analysis of sensory data that takes place in the cloud is the predominant use of AI software. AI is not a technology commonly built into the material objects – it is more often found in the cloud than at the edge.[54] The analysation of data is yet to reach its full potential. It is presently mostly reactive, rather than predictive and adaptive in a way where the system's outcomes are not predetermined.[55] This is partly due to the large computer power and network bandwidth required to perform adaptive actions.[56]

The current constrictions in computing capacity and bandwidth, as well as research shortage, mean that fully automated, predictive and adaptive IoT environments for consumers are not yet on the market. In other words, it is not possible to buy smart devices that act in unison to tailor all parts of a smart

[51] High-Level Expert Group on Artificial Intelligence, 'A definition of AI: Main capabilities and disciplines' (European Commission 2019), p. 6; see also Turner (2019), p. 16.

[52] The technical term for AI that changes its outcomes by synthesising insights from previous information is Machine Learning, which itself is a collective term for various intelligent technologies. The thesis will refer to self-learning AI instead of machine learning to keep technical terms to a necessary minimum. See for example Turner (2019), p. 61 for a definition of machine learning.

[53] High-Level Expert Group on Artificial Intelligence (2019) p. 1 and 6.

[54] Adi E, et al (2020), p. 4 and 40.

[55] Adi et al. (2020), p. 27f; Commission (2020), p. 7.

[56] Adi et al. (2020), p. 27.

home to the homeowner's needs and preferences without active human demand. The integration of AI and IoT is thus in its infancy. Moreover, most of the interest in increasing the use of self-learning AI in IoT contexts is directed at industrial applications.[57] Smart cities could for example predict and recommend optimal traffic routes through swarm intelligence.[58] In manufacturing, predictive AI could decrease the risk of machinery breakdown.[59]

AI and IoT is expected to intertwine further as technological limitations fade. The roll-out of 5G will play an important role as the high bandwidth of 5G will strengthen processing capacity and enable more IoT devices to connect to the internet. With more IoT devices comes more available data, as well as an incentive for companies to further develop the devices. In turn, the demand for artificial intelligence in IoT is predicted to increase.[60]

---

[57] Adi, E. et al. (2020), p. 6 and 8-17; see also 'Leveraging the upcoming Disruptions from AI and IoT: How Artificial Intelligence will enable the full promise of the Internet-of-Things' (PWC 2017).

[58] Zedadra O et al., 'Swarm Intelligence-Based Algorithms Within Iot-Based Systems: A Review' (2018) 122 Journal of Parallel and Distributed Computing, p. 179; Adi, E. et al. (2020), p. 28f; see also PWC (2017), p. 15.

[59] Adi et al. (2020), p. 28f; see also PWC (2020), p. 15.

[60] Barbero et al. (2018), p. 33f; 'The European Market Potential For (Industrial) Internet Of Things CBI' (*Cbi.eu*, 2021) https://www.cbi.eu/market-information/outsourcing-itobpo/industrial-internet-things/market-potential#:~:text=By%202024%2C%20Europe%20is%20expected,IoT%20devices%20in%20the%20world. accessed 20 May 2021.

3 The PLD

3.1 Introduction

This chapter gives an overview of the PLD's objectives and provisions. It begins with an account of the background and objectives of the PLD in chapter 3.2, which is necessary for in dept analyses throughout chapter 4 of how IoT fits within the EU's liability regime. A short presentation of the most important provisions is also presented herein. This is done to place the central notions of the PLD into context.

Thereafter, the notions of product and defect as well as the liability exemptions called the later defect defence and the development risk defence will be thoroughly examined in chapter 3.3 through 3.5. This information will constitute the basis on which chapter 4 is built.

3.2 Background, objectives and general provisions of the PLD

Product liability within the EU became harmonised in 1985 through the adoption of the PLD, creating a product liability regime that has been described as among the most important in the world.[61] The PLD created a system of strict liability for producers of defective products that cause damage.[62] Liability cannot be claimed for the defective product itself. The damage must instead take the shape of personal injury or material damage to another item of property that is ordinarily intended for private use or consumption, exceeding a

[61] See Rihtar K, 'Product Liability, Legal Transplants and Artificial Intelligence' (2019) harmonious, p. 293.

[62] PLD Article 1.

lower threshold of 500 ECU.[63] As the liability is strict, the injured person does not need to prove the producer's fault. However, it befalls the injured person to prove the damage, the defect and the causal relationship between defect and damage.[64] Article 11 establishes that the rights conferred upon the injured person are extinguished upon the expiration of ten years from the date on which the producer "put into circulation" the product, unless the injured person before that date has begun proceeding against the producer.[65]

The PLD takes the shape of a maximum harmonisation for product liability, seeking to ensure a coherent level of strict liability throughout the union.[66] However, there is not total unification of liability for defective products. The PLD does not aim to harmonise matters not regulated by it.[67] Most noticeably, the PLD's strict liability regime is complemented by national regulations of liability on other grounds, such as fault and warranty.[68] The importance of the PLD is not diminished by the non-harmonised rules. Only the PLD, through transposition into national law, sets the framework for liability without fault. There have been reports of discrepancy between the Member State's implementation of the PLD, although the PLD has substantially reduced the diversity of regimes that existed between Member States prior to the PLD's introduction.[69]

---

[63] PLD Article 9.

[64] PLD Article 4.

[65] See also PLD Article 10.

[66] Case C-52/00 *Commission of the European Communities v French Republic* EU:C:2002:252, para 24; Commission (2018c), p. xii.

[67] Case C-285/08 *Moteurs Leroy Somer v Dalkia France and Ace Europe* EU:C:2009:351, paras 24 and 25..

[68] Case C-402/03 *Skov Æg v Bilka Lavprisvarehus A/S and Bilka Lavprisvarehus A/S v Jette Mikkelsen and Michael Due Nielsen* EU:C:2006:6, para 47.

[69] Machnikowski P, *European Product Liability: An Analysis Of The State Of The Art In The Era Of New Technologies* (Intersentia 2016), p. 672.

The objectives of the PLD are, according to the first recital in the preamble, to ensure a uniform level of consumer protection, to avoid competition distortions and to strengthen the free movement of goods.[70] A crucial aspect of the PLD is striking a fair balance between the responsibilities of producers and consumers.[71]

It has been noted by scholars that the legal basis of better consumer protection as an objective for the PLD is questionable, as primary law at the time of the PLD's adoption did not explicitly see to the interests of consumers.[72] Indeed, the legal ground for the PLD is today's Article 113 TFEU, which authorises the creation of harmonising legislation where necessary to ensure the completion of the internal market. The PLD's emphasis on strengthening the free market through harmonisation is as a consequence of the limited scope of power available in 1985.[73] Today, however, consumer protection as a central objective of product liability goes undisputed.

The PLD as a consumer-oriented law is not least apparent from that it is often categorised as such by the EU.[74] The PLD thus makes up one part of the EU's framework of private laws aimed at protecting consumer rights.[75] Moreover, product liability should be understood as a complement to the EU's product safety framework.[76] While the latter sets up *ex ante* safety requirements and standards that products must conform to before being placed on the market,

---

[70] The terms "goods" and "products" are used interchangeably in EU legislation, see Snell J, *Goods And Services In EC Law: A Study Of The Relationship Between The Freedoms* (Oxford University Press 2005), p. 4. In this thesis, "product" will be used unless referring to legislation that denotes something as "goods".

[71]Machnikowski (2016), p. 100; see also Commission (2018c), p. 52.

[72] Machnikowski (2016), p. 680.

[73] Machnikowski (2016), p. 680.

[74] See for instance the EU's webpage, were the PLD has been listed among laws concerning consumer protection, 'Consumers - EUR-Lex' (*Eur-lex.europa.eu*, 2021) https://eur-lex.europa.eu/summary/chapter/09.html accessed 18 May 2021.

[75] European Law Institute (2021), p. 4.

[76] Commission (2020), p. 12.

product liability becomes relevant when a product was not as safe as it should have been and thus caused damage.[77] The PLD acts as a source of incentive for producers to create safe products, by allocating the economic burden on a producer whose product has caused damage to property or harm to a person.[78]

3.3 A closer look at "product"

One of the key notions of the PLD is "product". If what has caused damage through its defectiveness is not deemed a product, the PLD does not apply. Product is defined in Article 2:

> *For the purpose of this Directive 'product' means all movables, with the exception of primary agricultural products and game, even though incorporated into another movable or into an immovable. […] 'Product' includes electricity.*

The condition that a product must be movable has often been interpreted as meaning that only tangible goods constitute products.[79] If an object cannot be touched, it cannot be moved. Some departure from the tangibility requirement can be seen in that electricity is regarded as a product, despite being intangible. However, the fact that electricity is regarded as a product in the meaning of the PLD could be interpreted as a tangibility requirement for all products unless stated otherwise.[80]

Products should be distinguished from services. The latter are not covered by the PLD. This is not explicitly stated in the PLD, as services are not mentioned therein, but follows from the provisions *e contrario*. Both primary and

[77] Commission (2020), p. 12.

[78] Commission (2020), p. 12.

[79] See for example Commission (2018c), p. 74.

[80] Alheit K, 'The Applicability of the EU Product Liability Directive to Software' (2001) Comparative and International Law Journal of Southern Africa, p. 200; Rihtar (2019), p. 301.

secondary EU law has a general split between goods, i.e. products, and services. That services are not within the scope of the PLD has also been made unequivocally clear by case law.[81] Unfortunately, the court has not taken it upon itself to define services within the meaning of the PLD beyond the specific situations covered by the cases. Needless to say, there is less agreement regarding the definition of services than the definition of products.[82] This goes for the distinction between goods and services more generally within EU law too.[83] Even the TFEU defines services negatively, as an economic activity not governed by the provisions on goods, capital and persons.[84] Nonetheless, the intangibility aspect of services is often highlighted as a defining feature.[85] It has also been argued that services, in contrast to products, cannot be traded.[86]

3.4 A closer look at "defective"

3.4.1 Assessment of defect

An injured person must prove the defect of the product to claim liability. According to Article 6 of the PLD, a product is defective "when it does not provide the safety which a person is entitled to expect, taking all circumstances

[81] Case C-203/99 *Henning Veedfald v Århus Amtskommune* EU:C:2001:258; C-495/10; see also recital 1 and 9 of the preamble to the PLD.

[82] Hojnik J., 'Technology Neutral EU Law: Digital Goods Within the Traditional Goods/Services Distinction' (2016a) International Journal of Law and Information Technology, p. 65.

[83] For a thorough elaboration on the distinction between goods and services within EU primary law, see Snell (2005).

[84] TFEU Article 57.

[85] Case C-155/73 *Giuseppe Sacchi* EU:C:1974:40 p. 426f; Hojnik (2016a), p. 65.

[86] Hojnik (2016a), p. 65; see also Case 7/68 *Commission of the European Communities v Italian Republic* EU:C:1968:51, p. 428.

into account". Differently phrased, defectiveness stems from an abnormal potential for damage.[87] Absolute safety is not supported by the PLD.[88]

Article 6 further specifies the circumstances that must be taken into account in the assessment of defectiveness. Circumstances include, but are not limited to, the presentation of the product, the use to which it could reasonably be expected that the product would be put and the time when the product was put into circulation. Circumstances established by case law include, inter alia, the objective characteristics and properties of the product in question.[89] The mere fact that a better product has been put into circulation does not render the product defective, according to Article 6(2). In *Boston Scientific*, a case that dealt with defects in pacemakers and cardioverter defibrillators, the Court found that the function of those products and the vulnerability of the patients using them meant that patients were entitled to expect "particularly high" safety requirements.[90]

The wording of Article 6 makes clear that the assessment of the defectiveness of a product is made on the basis of the consumer expectation test.[91] More precisely, the assessment is based on the average consumer expectation test.[92] The subjective expectations of the injured person in question is irrelevant for

[87] Joined Cases C-503/13 and C-504/13 *Boston Scientific Medizinitechnik GmbH v AOK Sachsen-Anhalt and other* EU:C:2015:148, para 40; see also Borghetti, J-S, 'Civil Liability for Artificial Intelligence: What Should its Basis Be?' (2019) La Revue des Juristes de Sciences Po, p. 97.

[88] Mazzini G, 'A System of Governance for Artificial Intelligence through the Lens of Emerging Intersections between AI and EU Law' in A. De Franceschi - R. Schulze (eds.), *Digital Revolution – New challenges for Law* (Verlag C.H.Beck oHG 2019), p. 13.

[89] Joined cases C-503/13 and C-504/13, para. 38.

[90] Joined cases C-503/13 and C-504/13, para. 39.

[91] Alheit (2001), p. 196.

[92] Commission (2018c), p. 84.

the assessment. It is the expectations of the public at large that are the determining factor.[93] Thus, the test is objective.[94]

Defectiveness is commonly categorised into three types: manufacturing defects, design defects and information defects. This distinction is not supported by the PLD per se, but is common in for example American liability law and has been observed by the Commission to be applied in Member States too.[95] Manufacturing defects refer to instances where a specific product deviates from the intended design of the product.[96] In such cases, the entitled expectation is that all copies of a product adhere to the same standard.[97] Design defects occur when the design of a product renders it unreasonably dangerous.[98] When a producer has failed to adequately warn consumers of potential dangers of a product, it constitutes an information defects.[99] It can be noted that while a producer of the finished product can be held reliable for all types of defects, a component producers can only be held liable for manufacturing defects.[100]

In contrast to manufacturing defects, the two latter categories of defects cannot be compared to a predetermined standard. As the consumer expectation

[93] Recital 6 of the Preamble; See also Joined cases C-503/13 and C-504/13 para. 37.

[94] Mazzini (2019), p. 16.

[95] Wuyts D, 'The Product Liability Directive – More Than Two Decades of Defective Products in Europe' (2014) 5 Journal of European Tort Law, p. 10 and 12; Commission (2018c), p. 84.

[96] Alheit (2001), p. 196.

[97] Reutiman L, Defective Information: Should Informaiton Be a Product Subject to Product Liability Claims (2012) 22 Cornell Journal of Law and Public Policy, p. 198.

[98] TNO, 'Study on Safety of non-embedded software: Service, data access, and legal issues of advanced robots, autonomous, connected, and AI-based vehicles and systems: Final Study Report regarding CAD/CCAM and Industrial Robots' (European Commission 2019) p. 133.

[99] TNO (2019), p. 133.

[100] PLD Article 7(f).

test is normative rather than factual, it is courts which, on a case-by-case basis, assesses what degree of safety the public is entitled to expect.[101] Different legal tests of the assessment of defectiveness have emerged in courts due to the vague formulation provided by the PLD of when a product can be regarded defective.[102] The consumer expectation test is often carried out alongside other tests when design or information defects occur, such as the risk-utility test.[103] The greater difficulty for injured persons to prove design or information defects, compared to manufacturing defect, was somewhat eased by the precedent set in the case *Boston Scientific*. The Court ruled that a specific product can be classified as defective without establishing that it is defective as such, if it is found that all products of the same series have a potential defect.[104] This judgement underpins the preventive function of the PLD.[105]

3.4.2 Put into circulation

The producer is only liable for defects present at the time when the product was put into circulation. As such, put into circulation plays a key role in if a defect can lead to liability. Beyond being one of the conditions in Article 6, put into circulation can be found mainly in two other provisions, namely in the liability exceptions established in article 7 and the time limit on liability in article 11.

Despite it being a central notion, "put into circulation" is not defined in the PLD. A brief definition was given in the 1976 proposal for the PLD. It was explained that the relevant point in time is when the product enters the chain

[101] Wuyts (2014), p. 8f.

[102] Borghetti (2019), p. 97; Mazzini (2019), p. 17.

[103] Commission (2018c), p. 84.

[104] Joined cases C-503/13 and C-504/13 paras. 41 and 43.

[105] Joined Cases C-503/13 and C-504/13 *Boston Scientific Medizinitechnik GmbH v AOK Sachsen-Anhalt and other* EU:C:2015:148, Opinion AG Bot Y., para 38.

of distribution.[106] In the case C-127/04, concerning Article 11, the Court concluded that:

> *a product is put into circulation when it is taken out of the manufacturing process operated by the producer and enters a marketing process in the form in which it is offered to the public in order to be used or consumed.*[107]

In the case, the claimant argued that the putting into circulation of a product occurred when the producer lost control of that product.[108] The Court did not entirely dismiss this. If there is a close connection between the producer and a subsequent part of the distribution chain, e.g., a wholly owned subsidiary of the producer, a situation may arise where the transfer of the product from one to the other of those entities does not amount to putting the product into circulation.[109] However, the close link between different parts of the distribution chain is not conclusive in placing the moment of putting into circulation.[110]

The Court gave weight to two other aspects. It began by recalling earlier case law stating that the exceptions in Article 7 are to be interpreted restrictively in order to protect the interests of the victim.[111] Thereafter, it made an extensive interpretation of the 10th recital in the preamble.[112] The recital states that limiting the time period for taking action for compensation is in the interests of both the injured person and the producer. The Court interpreted this as meaning that Article 11, contrary to Article 7, is of a neutral character and

---

[106] Commission, 'Bulletin of the European Communities Supplement 11/76' (1976), p. 16.

[107] Case C-127/04, *Declan O'Byrne v Sanofi Pasteur MSD Ltd and Sanofi Pasteur SA.* EU:C:2006:93, para 32.

[108] C-127/04, para. 21.

[109] C-127/04, para. 29f.

[110] C-127/04, para. 31.

[111] C-127/04, para. 25.

[112] C-127/04, para. 26.

that the aim of Article 11 is to "satisfy the requirements of legal certainty in the interests of the parties involved."

Thus, the Court saw to the need of a clear point in time for "put into circulation" to occur, while acknowledging the variety of ways in how distribution chains can be constructed. A producer could risk postponing when the decisive moment occurs by remaining in control of the product, but the product is nonetheless in circulation when it is offered to the public. What remains somewhat unclear is if "put into circulation" has a different meaning when read in the context of Article 7 compared to Article 11. It does not seem this way, as the Court defines "put into circulation" as *one* concept, found in particular in Articles 7 and 11.[113] The Court also derived its interpretation by analysing the aim of both Article 7 and Article 11. If a discrepancy were intended, the judgement suggests that an interpretation that sees to the injured person's interests will be even higher valued when any of the defences in Article 7 are raised by the producer.

3.5 Liability exemptions despite defect

3.5.1 Generally about Article 7

Article 7 of the PLD provides an exhaustive list of conditions under which the producer can be cleared of liability, despite a product being defective. The exemptions must be interpreted strictly.[114] Two of these exemptions are particularly interesting where new technologies are concerned. First, the briefly mentioned exemption commonly referred to as "the later risk defence", found in Article 7(b), could arguably be put on its head due to widespread digitali-

[113] C-127/04, para 23.

[114] Case 203/99, para 15.

sation of material products. Second, it has been argued that the so called "development risk defence" in Article 7(e) might be used more extensively than initially intended due to rapid technological developments.[115]

3.5.2 The Later Defect Defence

A natural consequence of the necessary condition that a defect existed when the product was "put into circulation", is that producers cannot be held liable for defects that arise thereafter. A producer can, in accordance with Article 7(b), raise this as a defence against an injured person. The later defect defence is formulated as follows:

> *The producer shall not be liable as a result of this Directive if he proves:*
>
> *[…] (b) that, having regard to the circumstances, it is probable that the defect which caused the damage did not exist at the time when the product was put into circulation by him or that this defect came into being afterwards*

Hence, the exemption deals with situations where the cause of the defect does not lie with the producer. This is similar to Article 7(a), which primarily covers cases where someone else than the producer caused the product to leave the manufacturing phase,[116] thereby exposing the product to risks of defects that the producer had not intended for the consumer.

[115] Commission (2018c), p. 96.

[116] C-203/99 para. 16.

3.5.3 The Development Risk Defence

The inclusion of the development risk defence clause in Article 7(e) of the PLD was preceded by decades of debate.[117] While consumer associations were – and still are – of the opinion that the development risk defence could create gaps in consumer protection, producer associations highlighted the risk of decreased market innovation and the discouragement of scientific and technical research if the defence were to be excluded.[118] In the first draft of the PLD, published ten years prior to the PLD's adoption, producers could be held liable for development risks.[119] The final version of the PLD instead states that Member States can decide if their national legislation extend to development risk or not. Most Member States have implemented the liability exception.[120] Lengthy evaluations of the meaning and possible consequences of the development risk defence clause have been published ever since.[121]

The development risk defence can be found in Article 7(e), which states that:

> *The producer shall not be liable as a result of this Directive if he proves:*
>
> *[…] (e) that the state of scientific and technical knowledge at the time when he put the product into circulation was not such as to enable the existence of the defect to be discovered*

---

[117] Fondazione R, Analysis of the Economic Impact of the Development Risk Clause as Provided by Directive 85/374/EEC on Liability for Defective Products: Final Report (European Commission 2004), p. 19 and 21f.

[118] Fondazione (2004), p. 21, see also BEUC, 'Product Liability 2.0: How to make EU rules fit for consumers in the digital age' (2020), p. 20.

[119] Fondazione (2004), p. 19.

[120] Fondazione (2004), p. 28; Expert Group on Liability and New Technologies, 'Liability for Artificial Intelligence and other emerging digital technologies' (European Commission 2019), p. 28.

[121] See especially Fondazione (2004).

In other words, defects that have caused damage do not lead to liability if the producer can prove that the state-of-the-art knowledge at the time when the product was put into circulation could not have foreseen the existence of the defect.[122]

The leading ruling supplying guidance on the meaning of Article 7(e) is case C-300/95.[123] The court began by stating that "scientific and technical knowledge" is not limited to the producer's industrial sector – it extends to the most advanced level of scientific and technical knowledge in the scientific community as a whole.[124] The AG was more elaborate than the court when defining what falls within the concept of "state of knowledge". The AG-pointed out that scientific progress is not linear, as there can be opposing opinions on a newly discovered subject matter but that a passage of time leads to the matter being unanimously agreed upon within the community.[125] In the AG's view, the most advanced level of research does not translate to the view held by the majority within the community, but the entirety of studies and discoveries.[126]

Furthermore, the Court established that the producer's subjective knowledge is irrelevant. It is the objective state of scientific and technical knowledge that is relevant.[127] The producer is presumed to have been informed about the state-of-the-art knowledge. The knowledge must, however, have been accessible at the time when the product was put into circulation.[128] The Court was

[122] Expert Group on Liability and New Technologies (2014), p. 28f.

[123] Case C-300/95 *Commission of the European Communities v United Kingdom of Great Britain and Northern Ireland* EU:C:1997:255, para 26; Fondazione (2004).

[124] Case C-300/95, para 23.

[125] Case C-300/95, para 21.

[126] Case C-300/95, para 21.

[127] C-300/95, para 27.

[128] C-300/95, paras 28 and 29.

of the opinion that the accessibility of the knowledge was an implicit condition in the wording of Article 7(e).[129] Once again, the court followed the opinion of the AG, who highlighted that the opportunity for the information to be available to a producer in the EU should be of relevance in discerning if the development risk defence is applicable.[130] The AG stated that factors such as place of origin, language and the circulation of journals have implications for how easily available technical and scientific knowledge is.[131]

[129] C-300/95, para 28.

[130] Case C-300/95, para 23.

[131] Case C-300/95, para 23.

4 Product liability and IoT

4.1 Introduction

The previous chapters introduced IoT and covered the basics of the PLD, including the underlying goals and the relevant operational provisions of the PLD. This chapter combines the tech with the law.

The chapter will begin with determining if the digital elements of IoT fall within the notion of product, in part 4.2 and 4.3. Predictions for how the court or the legislator will interpret the role of software, cloud technologies etc within the frame of the PLD will be presented. In doing so, shortcomings of the notion of product will also be discussed.

Defect and the liability defences will then be evaluated. Chapter 4.4 will critically review one central aspect of the notion of defect, namely "put into circulation". This part will focus mostly on the characteristics of IoT that are at conflict with "put into circulation". As the later defect defence is closely tied to this, discussions of the defence are included in chapter 4.4. Chapter 4.4 will lead into chapter 4.5 and an examination of consumers' reasonable expectations regarding consumer IoT, which is another essential aspect of determining if a defect exist. Thereafter, in chapter 4.6, the possibility to invoke the development risk defence when IoT products because damage will be thoroughly examined.

4.2 Digital elements of IoT as products

4.2.1 General observations on digital elements as products

4.2.1.1 Intangible servitization

The requirement that a product be movable, and in practice tangible, raises questions regarding its applicability to IoT devices. The material elements of smart devices unquestionably fall within the definition of Directive's "product". It is less clear whether the same holds true for digital elements. Software, for example, is not movable or tangible *in itself*. Information is, by definition, intangible.[132] If software and other digital elements fall outside the notion of product, any digital malfunction or vulnerability that leads to material or physical damage will not be covered by the PLD. The lack of material presence is one aspect to the difficulty in describing software and other digital elements as falling within to the notion of product.

However, the difficulty is twofold. The role of the digital elements is also relevant in defining them as product or not. The market has for decades displayed a trend towards increasingly selling products and services as package deals.[133] The term "servitization" has been coined to describe the merger.[134] Though seldom explicitly referred to by the legislator, or in doctrine, the movement towards integration between services and products underlies much of the discussion being held about the status of digital content.[135]

---

[132] Commission (2018c), p. 174.

[133] Hojnik J, 'The Servitization of Industry: EU law implications and challenges' (2016b) 53 Common Market Law Review, p. 3.

[134] Vandermerwe S and Rada J, 'Servitization of Business: Adding Value by Adding Services' (1988) 6 European Management Journal, p. 315.

[135] Hojnik (2016b), p. 8; for an example where servitization has been implicitly addressed by the EU see Commission (2018c), p. 70.

The intangibility of digital elements and its possible role as both service and product guides this subsection. Its relevance does, in fact, not pertain only to the definition issue. Some observations that encompass all IoT digital elements should first be presented, before a detailed analysis of the distinction between different types of digital elements is carried out.[136] These observations provide an attempt to work around the non-material service characteristics of digital content by the application of principles, while staying within the wording and objectives of the PLD.

4.2.1.2 The essential nature

Software is an integral part of products with digital elements. As the Commission has phrased it: "[n]either a computer not a smartphone would be of particular use without software.[137] The same holds true for IoT objects. Yet, software in IoT objects differ from computer programmes and smartphone apps in one central aspect. The software in IoT objects can give instructions for mainly material actions based on the continuous information and instructions from data processing. [138] For example, some smart thermostats can autonomously adjust the heat, not just send temperature reports to a smartphone app. Hence, the integration between material and digital is even more intrinsically linked in everyday smart objects than in a computer.[139] Where the main objective of IoT software is the operation of the product, the information and instruction in the software could be seen as a means for the proper functioning of the material product.[140]

---

[136] See chapter 4.2.2 and 4.2.3.

[137] Commission (2020), p. 13.

[138] The Chander A, 'The Internet of Things: Both Goods and Services' (2019) 18 World Trade Review, p. 16f.

[139] Chander (2019), p. 16f.

[140] Alheit (2001), p. 199f.; see also European Law Institute (2020), p. 10.

When the delivery of a product is the essence of a service, e.g. the service of sending instruction, provisions on goods are applicable to the service too.[141] In Anglo-American law, this is called the "essential nature test".[142] This has been upheld as an argument for the applicability of the PLD to faulty software, when the objective of the software is to provide a product.[143] However, the test is not conclusive evidence that IoT software or other digital elements are products. The instances where the "essential nature test" has been used in CJEU have dealt with the free movement of goods in general and the removal of quantitative restrictions in particular.[144] The free movement of goods is but one of the PLD's objectives, alongside protecting consumer's and ensuring undistorted competition in the single market.[145]

Still, the Court has touched upon the essential nature test in two liability cases concerning hospital treatment, though not explicitly so.[146] In *Veedfald*, the Court ruled that a product has been put into circulation when a service provider, in the course of providing services, uses a defective product (produced by the service provider) that causes damage.[147] In the latter case, *Dutrueux*, the circumstances were similar but the question the Court had to consider was different. Here, the question was if the service provider, who was not the manufacturer of the product, could be held responsible for the damage cause by the defective product. The Court found that this fell outside the scope of

---

[141] C-158/94 *Commission of the European Communities v Italian Republic* EU:C:1997:500, para. 18.

[142] Alheit (2001), p. 199. The essential nature test displays similarities to "the measure at issue", used to determine if the GATT or GATS agreement should apply in WTO disputes, see Chander (2019), p. 19f for information on the concept.

[143] Triaille J-P, 'The EEC Directive of July 25, 1985 On Liability for Defective Products And Its Application To Computer Programs' (1993) 9 Computer Law & Security Review, p. 217f; Alheit (2001), p. 199f.

[144] See for example C-158/94 and Case C-275/92 *Her Majesty's Customs and Excise v Gerhart Schindler and Jörg Schindler* EU:C:1994:119.

[145] Recital 1 of the preamble; see also Commission (2018c), p. 6.

[146] C-203/99; C-495/10.

[147] C-203/99 para 18, compare with C-495/10 paras. 37 and 38.

the PLD. The injured person could, however, hold the producer of the defect product responsible.[148]

It was in both instances irrelevant that the defective product was used as a means to carry out a service. The service did not need to be defective. The PLD still applied to the damage caused by products. On the other hand, the cases concerned situations where it was clearly the product that was at fault and not the service, and where the service rather than the product was the reason for the use of the product.[149] The Court has not yet needed to elaborate on if reasoning in line with the essential nature test would be favoured when the defect lies in the service and the service is used to provide a product.

4.2.1.3 Functional equivalence

Another aspect that should be considered when determining if software, as well as other types of digital elements, fall within the scope of the PLD is the principle of functional equivalence. This has at one point even been suggested by the EU's Expert Group on Liability and New Technologies.[150] There exist some disagreement among scholars regarding what the principle exactly entails.[151] On a general level, the principle establishes that there ought to be equivalent legal burdens between activities that are alike, specifically between activates carried out online and offline.[152] The principle was for example engrained in the EU's 2015 to 2019 Single Digital Market strategy,

[148] C-495/10, para. 39.

[149] C-203/99 para 12; C-495/10 paras 11 and 20.

[150] Expert Group on Liability and New Technologies (2019), p. 43.

[151] For a comparison between different interpretations of the principle, see especially Veerpalu A, 'Functional Equivalence: An Exploration Through Shortcomings to Solutions' (2019) 12 Baltic Journal of Law & Politics.

[152] Reed C, 'Online and Offline Equivalence: Aspiration and Achievement' (2010) 18 International Journal of Law and Information Technology, p. 2.

through the often repeated goal of creating a "level playing field" between the online and offline environment.[153]

When it comes to IoT, software and AI capabilities have taken over processes that once were and can be carried out mechanically or by humans.[154] In accordance with the principle of functional equivalence, damages caused by defects in such digital technologies should be within the scope of the PLD. This is due to that the mechanical and manual equivalence would result in liability.[155] In other words, the principle aims at levelling material processes with non-material processes and, in doing so, also address that digital actions show similarities to human services. The abovementioned Expert Group went so far as to state that the PLD is applicable to digital elements of material products, as they share similar functions to material items existing at the time of the PLD's drafting.[156] They mentioned control apps, OTA updates and digital services.[157] The Expert Group unsurprisingly followed the Commissions trend of not elaborating on their statement.

The principle of functional equivalence has been criticised for not bringing about actual equivalence. For instance, online content is too multifaceted to correspond solely to a newspaper or magazine.[158] Likewise, digital elements have been described as not merely a mechanical component constituting a "subsidiary aspect" of IoT, but the main product.[159] The digital technologies present different opportunities and limits, not reflected in the interests governed by the pre-existing rules.[160]

---

[153] See for example Commission, 'A Digital Single Market Strategy for Europe' COM (2015), p. 2.

[154] European Law Institute (2021), p. 3; see also DeNardis (2018) p. 38.

[155] Expert Group on Liability and New Technologies (2019), p. 35.

[156] Expert Group on Liability and New Technologies (2019), p. 43.

[157] Expert Group on Liability and New Technologies (2019), p. 43.

[158] Reed (2010), p. 6 and 9.

[159] European Law Institute (2021), p. 10.

[160] Reed (2010), p. 7.

The principle does not necessarily mean that laws that existed prior to digital technologies should be automatically applicable to the new developments either. The more common approach is to create specific rules to accommodate the digital technologies and thereby create equivalence between how the online and offline world is regulated.[161] Stating that the PLD is *per se* applicable to software and other digital elements based on the principle of functional equivalence, as the Expert Group did, is thus an oversimplification.

Though both the principle of functional equivalence and the essential nature test seem at first promising in determining that the notion of product within the meaning of the PLD encompasses all software and even all digital elements of IoT, neither is conclusive evidence. The principle and the test are well established within EU legislation and case-law. Possibly, they can indicate how defects in software, cloud computing etc. will fit within the frame of the PLD. However, the different digital elements must be broken down to find more definitive answers.

4.2.2 Software pre-installed on the device

For many years, the only guidance on whether software part of the object from the outset is to be regarded as a product or not, came from a concise answer given by Lord Cockfield on behalf of the Commission in 1998. When asked whether the PLD applied to computer programs, he replied that "the PLD applies to software in the same way, moreover, that it applies to handicraft and artistic products."[162] Thus, Lord Cockfield was of the view that software was covered. The Commission has in the last few years revisited the

[161] Reed (2010), p. 2.E

[162] C114/42, Official Journal of the European Communities 8.5.89 https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=OJ:JOC_1989_114_R_0001_01&qid=1429892489522&from=EN accessed 18 May 2021.

subject of embedded software. Unfortunately, a trend among the EU reports has been that the subject is not elaborate on beyond stating that there is uncertainty. Exceptions exist. In 2018, the Commission stated that "for products which include software at the moment they were put into circulation by the producer, the PLD could address liability claims for damages caused by defect in this software."[163] In a 2020 report the Commission reaffirmed that "software steering the operations of a tangible product could be considered part or component of that product".[164] However, this trend towards defining the meaning of the PLD does not bring complete legal certainty. At best, the Commissions reports can be regarded as soft law that will influence the Member States' national application of the PLD or act as a source of interpretation in future CJEU cases on the matter.

Nevertheless, the Commission's statements are in line with the majority view among scholars. Among scholars it has often been reasoned, beginning in at least the 1990s, that the tangibility of software can be derived from the medium it is placed on.[165] Some scholars, however, go one step further than the Commission in its recent communications. The tangibility of software through the material medium has by some been proof of that software is a product in its own right.[166] The Commission has not classified software as a product. The statement made in 2020 instead defines software as a component. The same can be inferred by the 2018 statement. No provision in the PLD requires components to be movable.[167] By avoiding referring to software as a product – even when it is part of a smart device or other material object

[163] Commission, Commission Staff Working Document, 'Evaluation of 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' SWD (2018) 157 (2018a), p. 52.

[164] Commission (2020), p. 14.

[165] Gemignani M, 'Product Liability and Software' (1981) 8 Rutgers Computer & Technology Law Journal, p. 188; Triaille (1993), p. 218f; European Law Institute (2021), p. 5.

[166] Alheit (2001), p. 100.

[167] Machnikowski (2016), p. 701.

– it is possible that the Commission has intended to ward off a redefinition of what constitutes a product. The distinction between component and product is mostly theoretical, as an injured person can turn to both the producer of the finished product and the component producer in liability cases, as the producer of the finished product is reliable for the safety of the component parts too.

Though no case law has confirmed that software that comes pre-installed on a IoT device falls within the scope of the PLD, the scholarly examinations and especially the recent statements from the Commission indicate that this is the case. Indeed, one can wonder if some scholars have at times complicated the matter by trying to distinguish between the medium and the software that instructs the medium.[168] Moreover, software in a general sense has more than half a century of history.[169] That the CJEU has never ruled in cases regarding the be or not be of software as a product in the meaning of the PLD – in IoT devices or any other of the infinite product were software is indispensable – suggests that this is not an issue in practise. Considering all of this, the analysis will from now on rest on the assumption that pre-installed software in IoT objects is not at conflict with the concept of product and that a producer is liable for defects which can be traced to faulty pre-installed software.

4.2.3 Software updates

4.2.3.1 An intangible good?

Though software updates can fix bugs and security risk, new bugs and safety risks can unintentionally be introduced because of it.[170] The applicability of

[168] See for example Alheit (2001), p. 14.

[169] Zoeller et al. (2005), p. 746ff.

[170] Cabral T, 'Liability and Artificial Intelligence in the EU: Assessing the Adequacy Of The Current Product Liability Directive' (2020) 27 Maastricht Journal of European and Comparative Law, p. 624; European Law Institute (2021), p. 5.

the PLD to software becomes more complex when one looks at software updates. This is due to the increasing difficulty in distinguishing between products and services.[171]

The internet connection of IoT devices often makes it possible for the producer to install updates OTA. This is a set of technique much younger than that of combining software directly with a material product, one not available for example at the time Lord Cockfield made his assessment of software.[172] In contrast to software bought and installed as a CD-ROM or DVD, a software download online has no material elements attached to it.[173] Neither is it sold together with the material IoT object. Software updates are instead an addition to an IoT object, but the addition is not physically incorporated into the object in the same way that a mechanical component part is. Thus, it is questionable if OTA updates can be regarded as incorporated into an IoT object.[174] This suggests that updates should be regarded as maintenances carried out to improve the product, rather than a product or component.[175]

Yet, digital technology has altered one of the fundamental aspect of services. Even if software is regarded as a service, it can be stored digitally and trans-

---

[171] Hojnik (2016b), p. 4 and 8.

[172] For instance, in 2012 Tesla became the first company to do an OTA update of a car, see Byford S, 'Tesla Model S Getting First Ever Over-The-Air Car Firmware Upgrade Next Week' (*The Verge*, 2021) https://www.theverge.com/2012/9/24/3385506/tesla-model-s-over-the-air-car-firmware-update accessed 18 May 2021

[173] See for example, on the copyright of computer programs downloaded from the internet, Case C-128/11 *UsedSoft GmbH v Oracle International Corp.* EU:C:2012:407 paras 47 and 55.

[174] Chatzipanagiotis M., 'Product Liability Directive and Software Updates Of Automated Vehicles' (2020) Proceedings of SETN 2020 - 11th Hellenic Conference on Artificial Intelligence 2020, p. 2.

[175] Chatzipanagiotis (2020), p. 3.

ferred. The ability to transfer software makes it more akin to goods than services.[176] The Commission has, on the other hand, claimed that the possibility to duplicate software infinitely is a sign of intangibility.[177]

Tangibility has above been discussed as a necessary criterion for whether software – both updates and other software – falls within the scope of the PLD or not. However, this does not completely reflect the PLD. It follows explicitly from Article 2 that the notion of product includes electricity. Why then, could not software also be regarded as an intangible product? Electricity gained its status as a product, rather than a service, within EU law as the Court wished to put the energy sources oil, gas and electricity under the same provisions.[178] It is not unthinkable that the Court would value a uniform approach to material objects and software that steer the material objects like it has done with energy sources. Especially so for software updates, if both material objects and its pre-installed software are regarded as making up a product.

Moreover, though tangibility is inferred as a necessary condition unless otherwise stated in decades worth of doctrine, none of the PLD's provisions refer explicitly to tangibility. The word "tangible" has been treated as a synonym to movability, or at least a natural consequence.[179] This has neither been dismissed nor confirmed by the Court in product liability cases. Movable could very well be interpreted to include objects that are non-material.[180] In fact, some private law directives specify that they regulate only "tangible movable items", highlighting that a difference between the two terms exist.[181]

[176] Hojnik (2016a) p. 65.

[177] Commission (2018c), p. 174.

[178] Opinion of Mr Advocate General Fennelly Case C-97/98 para 20; Snell (2005), p.4.

[179] See for example Commission (2018c), p. 74.

[180] Rihtar (2019), p. 301.

[181] See especially Consumer Sales Directive 2019/771, Article 2(5)(a).

With this in mind, it is possible that the Court could rule that software updates fall within the notion of product. If the EU instead focuses greatly on tangibility as a distinguishing feature between goods and services, with electricity being a unique exception, the inclusion of software updates would likely require a broadening of the definition of product through a revision of the PLD.[182]

4.2.3.2 Entaglement of definitions

The definition of software updates as either product or service remains one of the unsolved questions in EU product liability. No substantial guidance can be found in neither the PLD nor relevant case law. The argumentations in doctrine and soft law are contradictory and inconclusive. Presently, the best indicator that software updates for IoT products should *de lege lata* be understood as falling within the notion of product, stem from the Commissions newfound willingness to discuss different types of software in connection with the notion of product.

Even the Commission's reports do, however, leave much to be desired. The aforementioned 2020 report combined the two related areas of product safety and product liability by referring to the former area of law in passing when discussing the latter.[183] Their short statement on software as a component in the meaning of the PLD did not differentiate between updates and software part of the initial product, but they were more elaborate regarding product safety. The Commission suggested that, within the meaning of product safety legislation, "software updates could be compared to maintenance operations."[184] This would render software updates a service, which falls outside the scope of product safety legislation. On the other hand, the Commission theorised that software updates that come with substantial alterations might

[182] Machnikowski (2016), p. 698 in conjunction with page 700f.

[183] Commission (2020), p. 13.

[184] Commission (2020), p. 10.

result in the entire product being regarded as a new product.[185] Updates that were foreseen by the manufacturer to be rolled out after the product was put on the market could, according to the Commission, also fall within the provisions of product safety legislation.[186] Software integrated into the product at the time of its placing on the market falls within product safety legislation.[187] How an assessment is to be carried out on whether a manufacturer foresaw an update or not is left unsaid in the report. Likewise, there are no instructions regarding how the distinction between small updates and substantial updates is to be made. In practice, the dichotomy between maintenance operations and substantial operations might not exist.[188]

The Commission does not clarify if their complex views on the difference between initial software and subsequent updates should apply to product liability too, beyond the call for a comparison made in the report. If this report were to influence future interpretations of the PLD, some software updates may be regarded as services, other updates as goods. At least one scholar has warned that oversimplification in how software is categorised in pre-digital era rules would lead to unwanted legal results.[189] An approach in line with the Commissions 2018 suggestions for software in regards to product safety rules could at least not be blamed for oversimplification. The risk is rather that it does not do away with legal uncertainty.

4.2.4 Networks and cloud computing – a cloudy area

The digital elements of IoT objects are not restricted to software. IoT is data-driven, utilises cloud and gateway technologies and wirelessly transmits and

[185] Commission (2020), p. 10

[186] Commission (2020), p. 11.

[187] Commission (2020), p. 10.

[188] Chatzipanagiotis (2020), p. 2.

[189] Hojnik (2016a), p. 83.

receive large amounts of data. The Commission has surprisingly paid much less attention to these aspects of IoT objects than it has on software.

For instance, in the 2018 working document evaluating the PLD, the Commission dwelled on cloud technologies explicitly for less than two paragraphs.[190] They addressed that the possibility to bundle together products and services makes it difficult to regard cloud computing as either one or the other.[191] The Commission did, however, also state that "[p]roviding data through an IoT system could be considered a service".[192] The provision of data is what cloud computing and IoT network connection is mainly concerned with.

Networks were briefly covered in another document from the same year. The report evaluated liability for autonomous vehicles and was carried out by the European Parliamentary Research Service on behalf of the European Parliament.[193] The focus did not lay on the definition of networks as products as such, but instead on consumer expectations. A scenario was painted up, where network interruption hindered essential data from being downloaded in time which causes an autonomous car to crash.[194] The writers argued that if "being connected is part of the package provided by the producer, then the car manufacturer is liable under the PLD for network problems, subject to the limitations and defences available under the PLD". [195]

As a person can only have safety expectations for the product, in accordance with Article 6, the statement indicates that network connection was in some scenarios regarded as a product or product component in the report. There is

[190] Commission, Commission Staff Working Document (2018a), p. 52 and 54.

[191] Commission, Commission Staff Working Document (2018a), p. 52.

[192] Commission, Commission Staff Working Document (2018a), p. 10.

[193] European Parliamentary Research Service, 'A common EU approach to liability rules and insurance for connected and autonomous vehicles' (European Commission 2018)

[194] EPRS (2018), 51.

[195] EPRS (2018), p. 25.

another possible reading. The decisive function of "package" is, like the problematisation of bundled products and services in the other report, a reference to servitization.[196] One could therefore interpret the argument as meaning that producers are liable for defects in services if the services are integral to the functioning of the product. As has been mentioned previously, the Court has never ruled in a liability case where a service that is used to provide a product, rather than the product itself, was at fault for damage caused. The writers reasoning does in fact seem to rely on the essential nature test, which does not have a history of support in product liability cases. [197]

The status of cloud and gateway computing and network connection as either part of or not part of the PLD is thus reliant upon the interpretation of what constitutes a service, mirroring the issue of software updates. The Commission's one sentence comment about data traffic is a strong indicator that these digital elements should be considered services. Furthermore, in its final report evaluating the PLD, the Commission conjectured that cloud computing is probably a service because of it being "run on remote servers".[198]

Yet, the Commission's assured stance was not evident throughout the final report. They more often noted the blurriness of the distinction between product and service regarding cloud computing.[199] The argument that cloud computing "does not seem to be a product" was brought up once, in a table annexed to the report, leaving the impression that the Commission aimed at burring the information.[200] The significance of the comment in the working paper can also be put into question based on its placement. It was made as part of information on the characteristics of emerging technologies.[201] That can be contrasted against the Commission's discussions on software as either service

[196] See Vandermerwe and Rada (1988), p. 316.

[197] See chapter 4.2.1.2.

[198] Commission (2018c), p. 175.

[199] Commission (2018c), p. 71f.

[200] Commission (2018c), p. 175.

[201] Commission, Commission Staff Working Document (2018a), chapter 5.4 and p. 52.

or product, which was carried out in connection with evaluations on different aspects of the PLD.[202] This disorganised handling of if damages caused by defects in cloud computing fall within the scope of the PLD highlight that the matter is not settled in soft law.

Looking beyond the Commission's definition attempts, the cloud could possibly be seen as supplying services based on the nomenclature used to explain it. Often, the infrastructure of the cloud is described as built up of Software as a Service, Platform as a Service and Infrastructure as a Service.[203] These three pillars have in common the carrying out of tasks remotely, i.e., removed from the material object, on virtual storage and platform spaces.[204] Some legal scholars seem to have adopted this technical categorisation, evidenced by them treating clouds as a service without explanation.[205]

More comprehensive analysis of data traffic as either service or product has been made regarding the law of the World Trade Organisation, where data traffic has been suggested to be a service within the meaning of the organisation's agreements based on dispute settlements on for example e-commerce.[206] Moreover, it was argued that smart object should be seen as a bundle of "both a good and an ongoing service", an opinion shared by two scholars who examined the PLD.[207]

The lack of discussion within the legal community is glaring. The only thing that seems certain is that the possibility to "bundle" is causing the established

---

[202] Commission (2020), chapter 3 and p. 13f.

[203] Barbero et al. (2018), p. 274; Adi et al. (2020) p. 6.

[204] See Barbero et al. (2018), p. 274.

[205] See for example Noto La Diega G and Walden I, 'Contracting for the 'Internet of Things': Looking into the Nest' (2016) Queen Mary School of Law Legal Studies Research Paper No. 219/2016, p.18; Cabral (2020), p. 619.

[206] Chander (2019), p. 18f.

[207] Chander (2019), p. 19.; Noto La Diega and Walden (2020), p. 15.

dichotomy of products and services to be too rigid to reflect market practises. More decisive information from the EU is needed to draw any conclusion on if these digital elements could fall within the notion of product when integrated into IoT objects. In fact, it is remarkable that the legal grey area of network failure has not enjoyed thorough examination already, as connectivity is so central to IoT that it is found in its name: *internet* of things.

4.2.5 Outlook to related areas of law

In the absence of information to determine if software updates and other digital elements that characterise IoT fall within the notion of product within the meaning of the PLD, one can look to consumer protection law in general and to the complementary area of product safety law in particular for guidance.

For instance, two sectorial safety legislations from 2017 have defined standalone software as a medical device and an *in vitro* diagnostic medical device, if the software is used for medical purposes.[208] The classification of standalone software in product safety law as a medical device if certain conditions are met goes back to 2007.[209] It has also been confirmed by case law.[210] In

[208] 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 [2017] OJ L 117/1, recital 19 of the preamble; Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU [2017] OJ L 117/176, recital 17 of the preamble.

[209] Directive 2007/47/EC of the European Parliament and of the Council of 5 September 2007 amending Council Directive 90/385/EEC on the approximation of the laws of the Member States relating to active implantable medical devices, Council Directive 93/42/EEC concerning medical devices and Directive 98/8/EC concerning the placing of biocidal products on the market [2007] OJ L 247/21, recital 6 of the preamble.

[210] Case C-329/16 *Syndicat national de l'industrie des technologies médicales (Snitem) and Philips France v Premier ministre and Ministre des Affaires sociales et de la Santé* EU:C:2017:947.

contrast to software updates that are downloaded to IoT objects, stand-alone software is, as the name suggests, sold without any material objects directly or indirectly connected to it. Thus, it is possible even for software with arguably fewer tangible aspects than OTA updates for IoT products to be regarded as products.

Another example, which more closely tangents that of liability for IoT products, is Directive 2014/53/EU (RED).[211] RED sets up safety and health requirements for radio equipment such as smart devices. It includes safety requirements for software that is "loaded into" radio equipment.[212] Only software that does not compromise the subsequent compliance of the radio equipment with applicable requirements should be able to be loaded into the radio equipment. Software is not explicitly defined as a product in RED. Instead, it is described as a component to radio equipment.[213]

The EU's adaptability to technical developments can be seen in other fields of consumer law too. The resent Sales of Goods Directive, a result of the Digital Single Market strategy, is an excellent example of this.[214] The Sales of Goods Directive regulates requirements concerning sales of goods concluded between sellers and consumers.[215] "Goods", i.e., products, is given a broad definition and includes goods with digital elements:

---

[211] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC [2014] OJ L 153/62.

[212] RED Article 3(i).

[213] RED Article 2 and 10(8), recital 30 of the preamble.

[214] 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 [2019} OJ L 136/28.

[215] Consumer Sales Directive 2019/771 Article 1.

> *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')*

By expanding the notion of goods to both digital content and digital services, the need to distinguish goods from service is removed. The intangibility of OTA updates, for instance, becomes irrelevant under the Sales of Goods Directive. This is in stark contrast to the dichotomy between goods and services under the PLD examined above. The Sales of Goods Directive does not limit itself to software, as the directives on medical devices and RED do. Cloud computing and continuous data traffic are among the types of digital elements that explicitly fall within the Sales of Goods Directive.[216]

It can also be noted that the Sales of Goods Directive does not denote digital elements to the status of components. In fact, it is the material parts of goods with digital elements that are referred to as components in the recitals.[217] This can be contrasted with the PLD, where the movability of products is highlighted but the state of components is not defined.

The provisions in these legislations do not translate into requirements under the product liability regime. Instead, the analogies can hint at the direction in which the EU might take regarding the matter. The main takeaway from the Sales of Goods Directive is the legislator's readiness to handle situations where servitization is apparent. The broad definition of goods within this directive could prove as inspiration if the Commission were to undertake a revision of the PLD.[218] Concerning safety legislation, the legislator's awareness that software must be regulated *ex ante* to prevent harm indicate that the EU will not disregard software in product liability cases.

---

[216] Directive 2019/771 recital 15 of the preamble.

[217] Directive 2019/771 recital 39 of the preamble.

[218] Cabral (2020), p. 621.

It should be pointed out that the Commission has argued that the explicit reference to software in safety legislation could be interpreted as an indication that it falls outside the scope of the PLD.[219] This fails to take into account that the PLD was adopted at a time prior to widespread use of integrated and stand-alone software, while the product safety regulations are from the 21st century.

4.2.6 Is an update called for?

At the time of its adoption, the PLD's notion of product was regarded as broad. The legislator was even aware, apparent from the second recital of the preamble, that an age of complex products had begun. There was an obvious intention to encompass *all* items industrially produced for consumers into the product liability regime. Yet, In the current wording of the PLD, many of the dynamic features of IoT products will possibly fall outside the notion of product. Defects caused by these features will therefore not be covered by the PLD. The regulatory competence will instead befall the Member States. The issue in case of such an interpretation of the PLD is a lack of adequate and uniform protection throughout the Union for products where the main risks for damage lie in the digital elements.[220] To exclude liability based only on the fact that a defect can originate in a way that was not envisaged at the creation of the maximum harmonisation PLD seems arbitrary.

A revision of the notion of product can be glimpsed just beyond the horizon. Not only has a revision been suggested in doctrine, but the Commission sees this possibility too.[221] The European Parliament has even published a draft report urging the Commission to assess whether a redefinition of the term

[219] Commission (2018c), p. 62.

[220] Cabral (2020), p. 621.

[221] Noto La Diega and Walden (2016), p. 29; Commission (2018c), p. 131f; Commission (2020), p. 16f; European Law Institute (2021), p. 5.

product in the meaning of the PLD is necessary.[222] It is only possible to speculate if a change would lead the PLD to encompass digital elements more akin to services, comparable to how it has been handled in the Sales of Goods Directive. Presently, however, what producers ought to be prepared for in case of damages caused by their IoT objects and what protection consumers can expect is uncertain. The shortcomings do not end at the narrow notion of product. Below, different aspects of the notion of defect are examined.

4.3 Putting IoT into circulation

4.3.1 Producer control and tweaking the timing

The concept of "put into circulation", which is closely tied to the notion of defect and the defences producers can raise to avoid liability for defects, might be the most difficult aspect of the PLD to join with the characteristics of IoT items. Examining this notion first is therefore a good basis before discussing defect as such.

IoT products are not static items. Digital content is introduced countless times throughout the product's lifetime. While the material aspects of an IoT object stays largely unchanged from the time the product is put into circulation, this is not the case for everything beyond the material. Producers can control products long after they enter the marketing process.[223] Case law of the CJEU has, however, made clear that producer control is not decisive in deciding when a product is put into circulation. The focus of the Court has instead been on creating a before and an after for when a product is finished.[224] The moment

[222] Draft report on Civil liability regime for artificial intelligence (2020/2014(INL)), p. 3f.

[223] Expert Group on Liability and New Technologies (2019), p. 42f.

[224] C-127/04; see also chapter 3.4.2.

of "put into circulation" takes place where production passes from the production phase into the marketing phase. This allows the producer to determine when they consider their product to be safe enough for the public.[225]

On the other hand, the aspect of control was only examined in regard to close relationships between different actors in the distribution chain. The Court did not give its opinion on if a stronger reliance on control should apply when defects have been caused by products with digital elements. It is still an open question if products that display continued producer control would lead the Court to focus more on producer control and thereby delay the point in time when "put into circulation" occurs.

Some scholars have highlighted the need for greater influence of the producer's control in determining the moment of put into circulation occurs, which ought to result in that the moment is at least pushed forward to when a consumer buys an IoT object.[226] The argument goes that products could gather data that is accessible to the producer even after leaving the manufacturing process, which could be used to track eventual defects that arise later on in the distribution chain.[227]

Pushing "put into circulation" forward to a later point in time to accommodate technological advances could possibly disregard the balancing of interests that guide the PLD. Granted, the exemptions from liability in Article 7 seek to protect the interests of the injured person by restrictive interpretation.[228] It is therefore not problematic that it will lie only in an injured person's interest that the capacity for a producer to invoke the later defect defence decreases. Yet, a greater reliance on a producer's control of a product will also affect the

[225] Wuyts (2014), p 22.

[226] See especially Luzak J, 'A Broken Notion: Impact of Modern Technologies on Product Liability' (2020) 11 European Journal of Risk Regulation, p 634 and 647.

[227] Luzak (2020), p. 647f.

[228] C-127/04 para. 25.

concept of put into circulation in the meaning of Article 11. As is clear from case law, all parties' interests are of relevance to why the ten year limitation period came about.[229]

4.3.2 Further issues of put into circulation

Even if the critical moment were to be pushed forward, the wording and intention of the PLD cannot be ignored. For the PLD's provisions to function as intended, a product must be regarded as put into circulation at *some* point in time. The later defect defence would be redundant if a product was never deemed to have been put into circulation despite being in the hands of a consumer. The heart of the issue does not lie in the details of when put into circulation occurs. It is the great importance placed upon "put into circulation" in the PLD that does not reflect the control a producer maintains after material products with digital elements enter the marketing process.

The consequence of the prevailing focus on "put into circulation" can clearly be seen with software updates if they fall within the notion of product. There are two possibilities to how software updates as a product could be handled by the PLD: they could either be regarded as one and the same product as the material object, or each update could be regarded as a product itself.

In the first scenario, the product will have been put into circulation when it enters the marketing phase. Eventual updates, however, must naturally be regarded as put into circulation upon their release. Despite updates being covered by the PLD, the updates will take place after the product was put into circulation.[230] An increased use of, e.g., the later defect defence can be expected as a result of this.[231] The defence would allow the producer to escape

[229] C-127/04 para. 26.

[230] Cabral (2020), p. 624; Chatzipanagiotis (2020), p. 4f; European Law Institute (2021), p. 10.

[231] European Law Institute (2019) p. 10.

liability in cases were software caused damage, if they can prove that the damage was likely the fault of updates. This outcome was most likely not intended by the legislator, as Article 7(b) protects against situations where the producer did not cause of the damage.[232]

Treating software updates as products separate from the initial product creates other clashes with the PLD.[233] Liability extinguishes, in accordance with Article 11, upon the expiry of a period of ten years from the date on which the product was put into circulation. Each update may therefore prolong the producer's liability for software used in combination with the material product.[234] Hence, the formulation of Article 11 could act as a disincentive for producers to innovate if software updates were separate products.[235] Moreover, updates overwrite the initial software, in a way where one cannot be held apart from the other.[236] Deciding for what software malfunction a producer is liable for will become increasingly difficult after the initial product has reached the expiry period.

To a consumer, the capacity to hold a producer liable or not for software defects could in some cases appear arbitrary. To a producer, keeping track of exactly when an update was released and how it interacted with already present software would become a nuisance.[237] Liability that does not clearly expire for the entire product – that is, the material as well as all digital elements – after ten years, could lead producers to face greater financial burdens when the extended strict liability make it difficult to get insurance.[238] Either way,

---

[232] See chapter 3.5.2

[233] Treating updates and upgrades as products themselves is suggested in, e.g., Navas S, 'Producer Liability For AI-Based Technologies in The European Union' (2020) 9 International Law Research, p. 79.

[234] Chatzipanagiotis (2020), p. 6.

[235] Chatzipanagiotis (2020), p. 6.

[236] Machnikowski (2016), p. 96; Chatzipanagiotis (2020), p. 3.

[237] Cabral (2020), p. 624

[238] Machnikowski (2016), p. 96.

the costs could end up being borne by the consumer.[239] Distinguishing between the initial software and every subsequent update could have the overall effect that downsides for both producers and consumers are introduced. The provision limiting the time a producer can be held liable sees to balance the consumer's and the producer's interests. Decreasing the protection of both parties while keeping the balance of interests intact cannot, however, have been the intention of the PLD.

A similar issue can emerge with self-learning AI. If cloud computing with self-learning AI is regarded as a component of the IoT device, the question of when the AI learned a certain behaviour becomes relevant. An unwanted behaviour in self-learning AI could stem from poor programming from the outset. [240] The later defect defence would therefore not be applicable. However, the behaviour could also be the result of the AI being poorly taught. The defect is under such circumstances introduced after the product was put into circulation. [241] This does not necessarily raise the same issue of maintained producer control as with software updates. The producer's impact on the real-time environmental data that the AI processed and adjusted from is minimal.[242] Yet, the difficulty in combining possible self-learning capabilities with the rigid notion of put into circulation remains. The possible increase in the use of the later defect defence could be a reason to change the PLD, so that self-learning capabilities and software are considered or so that the exemption does not apply to products that can be updated.[243]

[239] Alheit (2001), p. 194.

[240] Cabral (2020), p. 625.

[241] Cabral (2020), p. 625.

[242] Expert Group on Liability and New Technologies (2019), p. 28.

[243] Cabral (2020), p. 629; European Law Institute (2021), p. 10.

4.3.3 Wear and tear

It has been suggested that put into circulation should be revised due to the incompatibility between the concept and dynamic technologies.[244] Abandoning the concept of put into circulation, even if only for products with digital elements, requires caution. IoT objects have material aspect too. These are not subject to the same producer control or constant renewal as that of software, cloud computing and continuous data generation. The PLD does not regard wear and tear as a defect either.[245] Even though software can degrade and suffer from bad repairs, the changes in digital elements are not comparable to the natural wearing out through use of material products.[246] A clear point in time from which lowering expectations because of wear out of the material product can be determined, has stood the test of time.[247] A concept that replaces put into circulation would need to cater to both the degradation of material elements and the possibilities of improving digital elements.

4.4 Putting IoT to the test

The apparent shortcomings of "put into circulation" tie well into the heart of the assessment of defect, namely the consumer expectation test. As it was phrased in one article, the wording of the Directive assumes that a product is "a one-time supply".[248] This is further made clear through the provision from which it follows that a consumer must buy a new product if he or she wants a better, safer product. Hence, changing social expectations of a product's

[244] Navas (2020), p. 82; European Law Institute (2021), p. 4.

[245] Commission (1976), p. 16.

[246] Commission, Commission Fact Sheet, 'Digital contracts for Europe – Question & Answer MEMO/15/6265' (2015), p. 2; European Parliamentary Research Service (2018), p. 66.

[247] Commission (2018c), p. 26f.

[248] European Law Institute (2021), p. 7.

safety do not translate into changed legitimate expectations for products that have already reached the consumer.[249]

This is of relevance for both design and information defects in IoT objects. Are consumers entitled to expect bug fixes and security updates of software? Should the producer inform the consumer if monitoring of the product has shown that there are safety risks with the product? Should the consumer expect that the product is free from vulnerabilities? Should data generation and processing constantly be accurate and robust? Can the consumer expect the network connection needed for machine-to-machine communication to be stable? These are but some of the questions that can be raised about the expectations on the product.

A reading of the Directive's wording leads to the conclusion that consumers cannot expect any improvements of the products design or information after the cut-off point that takes place when the product has been put into circulation. Hence, the PLD does not, *de lege lata*, leave room for expectations of the kind suggested in the first two questions above.

One scholar has contested this, arguing that the safety that a consumer is entitled to expect encompasses the whole period the product will be used.[250] Newly arisen threats that are not attended to by the producer are therefore to be regarded as defects.[251] The scholar based his argument on the *Boston Scientific* case.[252] It seems that the scholar specifically referred to that the case firmly established the preventive function of the PLD, acting as proof that consumers are entitled to expect alterations to products if threats arise.[253] However, the design defect of the whole product series that was of concern

[249] Machnikowski (2016), p. 27.

[250] Machnikowski (2016), p. 702.

[251] Machnikowski (2016), p. 702.

[252] See chapter 3.4.1.

[253] Machnikowski (2016), p. 55 and 702.

in that case was present when the product was put into circulation.[254] While the case did state that the characteristics and properties of the product are circumstances that must be regarded when assessing defect, that cannot overtrump the consideration of other circumstances – such as the time the product was put into circulation.[255]

The clear provisions of the PLD have not stopped legal scholars from suggesting that specific requirements *should* be expected of products that can be altered. It has been reasoned that there might be public interest in allowing consumers to expect continuous safety improvements, though such rights should be weighed against the producer's commercial interests.[256] Indeed, the ability and hence responsibility to send out updates to all objects affected by a safety risk could be regarded as a continuation of the ruling in the *Boston Scientific* case. Yet, software is never bug free, which begs the question of how safe the updated software should be if safety updates became a requirement.[257]. Absolute safety is not a reasonable expectation. A weighing of interests would thereby be necessary based on this too. It should also be pointed out that even the level of safety consumers can reasonably expect for preinstalled software – which does fall within the scope of the Directive – is so far an unsettled matter.[258]

Expectations on continuous information about safety risks, i.e., a broadening of when an information defect exists, may also be called for. The counterargument against this is that the information may be so complex due to the in-

[254] C-503/13, para. 14.

[255] Compare joined cases C-503/13 and C-504/13, para. 38 and PLD Article 6(1).

[256] Machnikowski (2016), p. 702; Mazzini (2019), p. 19f; see also Barbero et al. (2018), p. 122, who consider if a product could be regarded as defective simply because it cannot be updated.

[257] Alheit (2001), p. 204; see also Barbero et al. (2018), p. 121.

[258] Triaille (1993), p. 220.

nate complexity of the digital technologies, that the information does not increase the consumers understanding of the risk of defects.[259] Moreover, mere information and monitoring would not change the cause of the issue, as a consumer cannot reprogram the IoT object's software to wade of the risks.[260] An alternative way to improve information, while staying within the constraints of the PLD, would be to use the insights from IoT data to personalise labels on products.[261] This could have the positive effect that consumer are more well informed about the safety risks of products purchase.[262]

Irrespective of scholars theoretical reasoning, update requirements – both information updates and software updates – have already found their way into the Sales of Goods Directive. Article 7(3) of the directive provides that:

> *In the case of goods with digital elements, the seller shall ensure that the consumer is informed of and supplied with updates, including security updates, that are necessary to keep those goods in conformity [with the purposes for which goods of the same type would normally be used], for the period of time […]*

Just as this directive's definition of goods has been upheld as an inspiration for a revision of the PLD,[263] so could this provision foreshadow what a move towards incorporation of servitization into the PLD may result in.

There have also been suggestions on precise safety expectations regarding internet connection. As opposed to updates, the network stability is not intended to change throughout the products lifetime. In the study on autono-

[259] Chatzipanagiotis (2020), p. 4.

[260] Machnikowski (2016), p. 702.

[261] Luzak (2020), p. 635ff.

[262] Luzak (2020), p. 645.

[263] European Law Institute (2021), p. 5.

mous vehicles carried out on behalf of the European Parliament, it was suggested that consumers may reasonably expect a back-up system for network failures or warnings prior to the defect in the vehicle occurring.[264] It was further theorised that a consumer might be entitled to expect the autonomous vehicle to automatically park at an appropriate place.[265] The researchers were of the view that these expectations would only be reasonable if the network connection was "an integral part of the 'package' offered by the producer".[266] As discussed previously, the statement could be interpreted as arguing for an extension of safety expectations to services that are essential to the functioning of the product.[267] Such a change in scope of the PLD could not be carried out without a revision. The presence of any entitled expectations regarding the digital elements needed for continuous data-traffic is thus presently reliant upon them being categorised as products.

Even if consumers are intitled to expectations on the entire "package" of a product with digital elements and even if update requirements on software and information were introduced, the risk profile of the product is relevant in determining what a consumer is entitled to expect. As case law has made clear, products that have a high risk of causing severe damage if defects do occur entitle consumers to high safety expectations.[268] Consumer IoT that is confined to the user's home is not likely to cause as much damage as sophisticated autonomous vehicles or IoT used as part of e.g. infrastructure.[269] This means that, while network outages and neglected safety updates could be regarded as a defect for an automated vehicle, the same may not hold true for a connected refrigerator.

[264] EPRS (2018), p. 64.

[265] EPRS (2018), p. 64.

[266] EPRS (2018), p. 64.

[267] See chapter 4.2.4.

[268] Joined cases C-503/13 and C-504/13, para. 39.

[269] Barbero et al. (2018), p. 110f.

4.5 State-of-the-art IoT

Finally, the Commission has cautioned an eventual increase in the use of the development risk defence. The Commission envisions, though without detailed explanations, that producers will rely more often on the exemption as technologies become more complex.[270] At least in regard to consumer IoT products, this fear is not supported by case law.

Not only are the liability defences in general to be interpreted narrowly, but the case C-300/95 established that the threshold for the development risk defence to be applicable is high.[271] In contrast, the present shortcomings of IoT are well documented. That a specific threat does not materialise until after the product was put into circulation should not per se make the exemption applicable, as the general vulnerability for e.g. hacking should have been foreseen.[272] To paraphrase security advisor Everette, in the context of her discussing poorly designed and insecure IoT software, software designers have experience while companies that have recently begun creating IoT product lack that background.[273] Moreover, the "sell now, patch later" attitude prevalent on the software market leave possible security and safety flaws open after the product was put into circulation. The defects and damages that are brought about by the disregard for safety are design defect that cannot be explained away with reference to the development risk defence. The limited knowledge of a producer who has designed a product with defects is irrelevant when the state-of-the-art knowledge in the meaning of Article 7(e) is assessed.

[270] See for example Expert Group on Liability and New Technologies (2019). p. 29; Commission (2020), p. 15.

[271] See chapter 3.5.2.

[272] Machnikowski (2016), p. 701f.

[273] Knox Everette (2016).

Further still, IoT is not limited to consumer use. IoT also has industrial applications.[274] As state-of-the-art knowledge encompasses the most advanced level of knowledge in the scientific community as a whole, it is not implausible that insights from the field of industrial IoT will be relevant in product liability cases where the development risk defence is invoked.[275] Neither is IoT a breakthrough digital technology without connection to more well-established technologies. IoT expands upon building blocks present in other objects, such as smartphones, communication platforms and stand-alone software.[276] This too might present applicable information to producers of complex IoT products. One obstacle could be that a lot of research and development is being carried out in China, generating papers not easily accessible to European companies.[277]

It should be noted that the Commission's views are not tied directly to IoT products but to AI, or AI used as part of IoT.[278] As has been presented in this thesis, the full potential of AI is yet to reach the IoT market. Possible liability exemption complications brought about by self-learning AI incorporated into IoT are yet largely theoretical. The risks associated with self-learning AI can also be expected to be much greater when the IoT is not contained to a home or a single consumer.[279] The aforementioned research into automatic traffic lane recommendation in smart cities is an example of developments that could potentially cause more large-scale damage than interconnected wearables and smart homes could.[280] A future proof liability regime might need to bring about changes in this provision. As of now, however, consumers do not need to fret.

---

[274] See chapter 1.3.

[275] Rithar (2019), p. 302.

[276] DeNardis (2018), p. 44ff.

[277] Cabral (2020) p. 623.

[278] Expert Group on Liability and New Technologies (2019), p. 29.

[279] Barbero et al. (2018), p. 109ff.

[280] Barbero et al. (2018), p. 110f.

5 Conclusion

The purpose of this thesis has been to evaluate how two of the central notions of the PLD, namely product and defect, relate to IoT objects. After having assessed the relevant provisions of the PLD, the main characteristics of consumer IoT as well as the risks brought about by these characteristics, the conclusion is that the current legislation does not comprehensively regulate IoT objects.

Firstly, the notion of product is potentially too narrow to encompass all the digital elements that are integrated into IoT objects. It is likely that software that is part of the product when it was put into circulation is a component of the product. It is less certain if this holds true for the other digital elements intertwined with IoT objects. This is due to the difficulty in pinpointing where the dividing line between product and service should be drawn for digital elements united in intangibility. The thesis has shown that intangibility and the notion of service are two sides of the same coin. The bundling of tangible products and intangible services is thus the aspect of IoT objects that is the most difficult to combine with the PLD's rigid focus on products solely.

Though there exists some room for interpretation by the Court regarding the central notions of the PLD, it might be too much of a stretch to let intangible digital elements fall within the notion of product in the current wording of the PLD. The intertwining of parts that share similarities with products and parts that share similarities with services makes the categorisation as either one or the other difficult. This affects not only software updates, but also elements such as network connectivity and cloud computing. To what extent producers can be held strictly liable for network failures and malfunctions in data accuracy, for instance, is reliant upon on whether the digital elements are regarded as products.

Secondly, producers cannot be expected to introduce changes to the product after it has been put into circulation. If a producer does update an IoT object,

any bugs that were introduced through the new software and cause damage will not result in liability under the PLD. Neither is the producer required to send out instructions about a product's safety after the product was put into circulation. The increased producer control brought about by continuous connectivity of products is thus not addressed by the PLD. On the other hand, producers cannot easily escape liability by stating that a defect present when the product was put into circulation was unforeseen. The threshold for using the development risks defence is high, meaning that sophisticated digital technologies do not automatically result in no producer liability.

The thesis has presented that he PLD needs to be amended in order for consumers to enjoy protection for IoT objects on a par with that of traditional products. However, a revision where digital elements that share great similarities with services are inferred to have tangible aspects, through some vague connection to a material object, is at risk of creating a legal notion of product far removed from what it stood for when the PLD was adopted. It is questionable if the distinction between products, on the one hand, and services, on the other, is appropriate in a world moving towards more servitization. For the PLD to stay future proof, an acceptance that products with digital elements consist of *both* content and services is advisable. There are multiple indications that the PLD will be broadened in such a way. Indeed, it has already been achieved in other areas of consumer protection. Entitlement to safety expectations on the service elements of IoT objects would be a first step in creating protection on par with the liability regime for traditional, unconnected products.

As the PLD in its present state shows blatant shortcomings by basing the notion of defect on the moment a product was put into circulation, a revision aimed at establishing consumer protection for IoT objects would also need to switch focus to encompass a more dynamic evaluation of safety and defectiveness. The pressure from legal scholars on the EU in this regard is apparent. However, effectively changing this is a difficult task. The PLD must continue to be relevant for material products too. A revision of the notion of defect and

the provisions on liability exemptions will also require caution to get the balance right between consumer and producer interests.

An alternative way to tackle the diverging characteristics of traditional products, which are static by nature, and digitally equipped products, which are bundled together with services and can respond to the environment, is to create partially or entirely separate liability rules for the latter. The protection of the consumer would thereby be updated to reflect the modern technically advanced market.

Creating a separate liability regulation for IoT products does not go well with the spirit of the PLD. The technological neutral nature of the PLD was put in place to make it durable in an increasingly technically advanced world. Moreover, technical neutrality created a liability regime that, at the time of its adoption, aimed at encompassing all products used by consumers that caused damage. The horizontal approach to product liability made it uncomplicated for both consumers and producers – as well as other entities that could be held responsible for product malfunctions – to understand their respective rights and responsibilities. It was one law which established strict liability, not a scattering of regimes for different types of products. Indeed, the PLD was created to reduce the number of liability regimes that existed in the Union. The maximum harmonisation pursued under the PLD highlights this aspect even further. Introducing separate provisions for digital products, that do not fall neatly within the concepts established by the PLD, would be counteractive to the unity across markets that the PLD has sought to establish. The lines that can be drawn between tangible and intangible, goods and services, control or no control, have changed in a way that was unforeseeable in the 1970s and 1980s. What has not changed are the objectives of the PLD.

Time will tell if a revision is carried out or not. Presently, the unique characteristics of IoT objects largely fall outside the scope of the PLD. This leaves producers without a common regime to rely on and consumers with questionable product protection.

Bibliography

Legislation

Primary legislation

Consolidated Version of the Treaty on European Union (TEU) [2008] OJ C115/13.

Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union (TFEU) [2016] OJ C202/1,

Secondary Legislation

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 [1985] OJ L 210/29.

Directive 2007/47/EC of the European Parliament and of the Council of 5 September 2007 amending Council Directive 90/385/EEC on the approximation of the laws of the Member States relating to active implantable medical devices, Council Directive 93/42/EEC concerning medical devices and Directive 98/8/EC concerning the placing of biocidal products on the market [2007] OJ L 247/21

Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC [2014] OJ L 153/62.

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 [2017] OJ L 117/1.

Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU [2017] OJ L 117/176.

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 [2019} OJ L 136/28.

Commission communications and other documents

Barbero M, Cocoru D, Graux H, Hillebrand A, Linz F, Osimo D, Siede A, Wauters P, 'Study on Emerging Issues of Data Ownership, Interoperability, (Re-)usability and Access to Data, and Liability' (European Union 2018)

Commission, 'Bulletin of the European Communities Supplement 11/76' (1976).

Commission, Commission Fact Sheet, 'Digital contracts for Europe – Question & Answer MEMO/15/6265' (2015).

Commission, 'A Digital Single Market Strategy for Europe' COM (2015) 192 final.

Commission, Commission Staff Working Document, 'Evaluation of 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' SWD (2018) 157 final. (2018a)

Commission, Commission Staff Working Document, 'Liability for emerging digital technologies', SWD (2018) 137 final. (2018b)

Commission, 'Evaluation of Council Directive 85/374/EEC on the approximation of laws, regulations and administrative provisions of the Member States concerning liability for defective products - Final report' (2018c)

Commission, ‘Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics’ COM (2020) 64.

European Parliamentary Research Service, ‘A common EU approach to liability rules and insurance for connected and autonomous vehicles’ (European Commission 2018)

Expert Group on Liability and New Technologies, ‘Liability for Artificial Intelligence and other emerging digital technologies’ (European Commission 2019)

Fondazione R, Analysis of the Economic Impact of the Development Risk Clause as Provided by Directive 85/374/EEC on Liability for Defective Products: Final Report (European Commission 2004)

High-Level Expert Group on Artificial Intelligence, 'A Definition Of AI: Main Capabilities and Disciplines' (European Commission 2019)

TNO, ‘Study on Safety of non-embedded software; Service, data access, and legal issues of advanced robots, autonomous, connected, and AI-based vehicles and systems: Final Study Report regarding CAD/CCAM and Industrial Robots’ (European Commission 2019)

Books

DeNardis L, *The Internet in Everything: Freedom and Security in A World With No Off Switch* (Yale University Press 2020),

Hettne J and Otken Eriksson I, *EU-Rättslig Metod: Teori Och Genomslag I Svensk Rättstillämpning* (2nd edn, Nordstedts Juridik 2011).

Mazzini G, ‘A System of Governance for Artificial Intelligence through the Lens of Emerging Intersections between AI and EU Law’ in A. De Franceschi - R. Schulze (eds.), *Digital Revolution – New challenges for Law* (Verlag C.H.Beck oHG 2019).

Machnikowski P, *European Product Liability: An Analysis of The State Of The Art In The Era Of New Technologies* (Intersentia 2016).
Nääv M and Zamboni M, *Juridisk metodlära* (2nd edn., Studentlitteratur, 2018).

Sandgren, Claes, "*Rättsvetenskap för uppsatsförfattare: Ämne, material, metod och argumentation*" (4th Edition, Nordstedts Juridik, 2018).

Snell J, *Goods and Services in EC Law* (Oxford University Press 2005).

Turner J, *Robot Rules: Regulating Artificial Intelligence* (Palgrave Macmillan 2019).

Articles

Adi E, Anwar A, Baig, Z A., and Zeadally S, 'Machine Learning and Data Analytics for The Iot' (2020) 32 Neural Computing and Applications.

Alheit K, 'The Applicability of the EU Product Liability Directive to Software' (2001) Comparative and International Law Journal of Southern Africa.

Alter K, Dehousse R, and Vanberg G, 'Law, Political Science and EU Legal Studies' (2002) 3 European Union Politics.

Bauwens J et al., 'Over-The-Air Software Updates in The Internet of Things: An Overview of Key Principles' (2020) 58 IEEE Communications Magazine.

BEUC, 'Product Liability 2.0: How to make EU rules fit for consumers in the digital age' (2020).

Borghetti, J-S., 'Civil Liability for Artificial Intelligence: What Should its Basis Be?' (2019) La Revue des Juristes de Sciences Po.

Cabral T, 'Liability and Artificial Intelligence in the EU: Assessing the Adequacy Of The Current Product Liability Directive' (2020) 27 Maastricht Journal of European and Comparative Law.

Chander A, 'The Internet of Things: Both Goods and Services' (2019) 18 World Trade Review.

Chatzipanagiotis M., 'Product Liability Directive and Software Updates of Automated Vehicles' (2020) Proceedings of SETN 2020 - 11th Hellenic Conference on Artificial Intelligence 2020.

Dean B, 'An Exploration of Strict Products Liability and The Internet of Things' [2018] SSRN Electronic Journal.

European Law Institute, 'Guiding Principles for Updating the Product Liability Directive for The Digital Age' (2021),

Gemignani M, 'Product Liability and Software' (1981) 8 Rutgers Computer & Technology Law Journal.

Hessel S and Rebmann A, 'Regulation of Internet-of-Things cybersecurity in Europe and Germany as exemplified by devices for children' (2020) International Cybersecurity Law Review.

Hojnik J, 'Technology Neutral EU Law: Digital Goods Within the Traditional Goods/Services Distinction' (2016) International Journal of Law and Information Technology. (2016a)

Hojnik J, 'The Servitization of Industry: EU law implications and challenges' (2016) 53 Common Market Law Review. (2016b)

'Leveraging the upcoming Disruptions from AI and IoT: How Artificial Intelligence will enable the full promise of the Internet-of-Things' (PWC 2017).

Luzak J, 'A Broken Notion: Impact of Modern Technologies on Product Liability' (2020) 11 European Journal of Risk Regulation.

Navas S, 'Producer Liability For AI-Based Technologies In The European Union' (2020) 9 International Law Research.

Noto La Diega G, ‘Clouds of Things: Data Protection and Consumer Law at the Intersection of Cloud Computing and the Internet of Things in the United Kingdom’ (2016) 9 Journal of Law and Economics Regulation.

Noto La Diega G and Walden I, ‘Contracting for the ‘Internet of Things’: Looking into the Nest’ (2016) Queen Mary School of Law Legal Studies Research Paper No. 219/2016.

Reed C, 'Online And Offline Equivalence: Aspiration And Achievement' (2010) 18 International Journal of Law and Information Technology.

Reutiman L, Defective Information: Should Informaiton Be a Product Subject to Product Liability Claims (2012) 22 Cornell Journal of Law and Public Policy.

Riesenhuber K, *European Legal Methodology* (Intersentia 2017).

Rihtar K, 'Product Liability, Legal Transplants and Artificial Intelligence' (2019) harmonious.

Snyder F, 'The Effectiveness of European Community Law: Institutions, Processes, Tools and Techniques' (1993) 56 The Modern Law Review.

Snyder F, ‘Interinstitutional Agreements: Forms and Constitutional Limitations’ (1994) European University Institute.

Stefan O A, Avbelj M, Eliantonio M, Hartlapp M, Korkea-aho E and Rubio N, 'EU Soft Law in The EU Legal Order: A Literature Review' (2019) SSRN Electronic Journal.

Triaille J-P, 'The EEC Directive Of July 25, 1985 On Liability For Defective Products And Its Application To Computer Programs' (1993) 9 Computer Law & Security Review.

Tschider C, 'Regulating the Internet of Things: Discrimination, Privacy, And Cybersecurity In The Artificial Intelligence Age' (2018) SSRN Electronic Journal.

Vandermerwe S and Rada J, 'Servitization Of Business: Adding Value By Adding Services' (1988) 6 European Management Journal.

Veerpalu A., 'Functional Equivalence: An Exploration Through Shortcomings to Solutions' (2019) 12 Baltic Journal of Law & Politics.

Wuyts D, 'The Product Liability Directive – More Than Two Decades of Defective Products In Europe' (2014) 5 Journal of European Tort Law

Zedadra O, Guerrieri A, Joandeau N andSpezzano G, 'Swarm Intelligence-Based Algorithms Within Iot-Based Systems: A Review' (2018) 122 Journal of Parallel and Distributed Computing.

Zoeller F E, McMullin A, Hurd S N, Shears P, 'More Soft Landings for Software: Liability for Defects in an Industry That Has Come of Age' (2005) 21 Santa Clara High Technology Law Journal.

Websites

Byford S, 'Tesla Model S Getting First Ever Over-The-Air Car Firmware Upgrade Next Week' (*The Verge*, 2021) https://www.theverge.com/2012/9/24/3385506/tesla-model-s-over-the-air-car-firmware-update accessed 18 May 2021.

C114/42, Official Journal of the European Communities 8.5.89 https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=OJ:JOC_1989_114_R_0001_01&qid=1429892489522&from=EN accessed 20 May 2021.

'Consumers - EUR-Lex' (*Eur-lex.europa.eu*, 2021) https://eur-lex.europa.eu/summary/chapter/09.html accessed 18 May 2021.

Hay Newman L, 'An Elaborate Hack Shows How Much Damage Iot Bugs Can Do' (*Wired*, 2021) https://www.wired.com/story/elaborate-hack-shows-damage-iot-bugs-can-do/ accessed 18 May 2021.

Knox Everette W, 'Security Vulnerabilities, The Current State Of Consumer Protection Law, & How IOT Might Change It' (*Youtube*, 2016) https://www.youtube.com/watch?v=EFGcZwjw9Q4 accessed 18 May 2021

Lucian Constantin B, 'Hackers found 47 new vulnerabilities in 23 IoT devices at DEF CON' (*Computerworld*, 2016) https://www.computerworld.com/Article/3118762/hackers-found-47-new-vulnerabilities-in-23-iot-devices-at-def-con.html accessed 18 May 2021.

Lueth K, 'State Of The Iot 2020: 12 Billion Iot Connections, Surpassing Non-Iot For The First Time' (*IoT Analytics*, 2021) https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/ accessed 18 May 2021.

Parks Associates, 'Parks Associates: 33% Of Smart Home Device Owners Report Increased Usage During The COVID-19 Pandemic' (*Prnewswire.com*, 2021) https://www.prnewswire.com/news-releases/parks-associates-33-of-smart-home-device-owners-report-increased-usage-during-the-covid-19-pandemic-301197501.html accessed 20 May 2021.

'The European Market Potential For (Industrial) Internet Of Things | CBI' (*Cbi.eu*, 2021) https://www.cbi.eu/market-information/outsourcing-itobpo/industrial-internet-things/market-potential#:~:text=By%202024%2C%20Europe%20is%20expected,IoT%20devices%20in%20the%20world. accessed 20 May 2021.

Table of Cases

Court of Justice of the European Union

Case C-14/83, *Sabine von Colson and Elisabeth Kamann v Land Nordrhein-Westfalen* EU:C:1984:37.

Case C-322/88 *Salvatore Grimaldi v Fonds des maladies professionnelles* EU:C:1989:646.

Case C-275/92 *Her Majesty's Customs and Excise v Gerhart Schindler and Jörg Schindler* EU:C:1994:119.

Case C-300/95 *Commission of the European Communities v United Kingdom of Great Britain and Northern Ireland* EU:C:1997:255.

C-158/94 *Commission of the European Communities v Italian Republic* EU:C:1997:500.

Case C-203/99 *Henning Veedfald v Århus Amtskommune* EU:C:2001:258.

Case C-52/00 *Commission of the European Communities v French Republic* EU:C:2002:252.

Case C-136/04 *Deutsches Milch-Kontor GmbH v Hauptzollamt Hamburg-Jonas* EU:C:2005:716.

Case C-402/03 *Skov Æg v Bilka Lavprisvarehus A/S and Bilka Lavprisvarehus A/S v Jette Mikkelsen and Michael Due Nielsen* EU:C:2006:6.

Case C-127/04, *Declan O'Byrne v Sanofi Pasteur MSD Ltd and Sanofi Pasteur SA.* EU:C:2006:93.

Case C-285/08 *Moteurs Leroy Somer v Dalkia France and Ace Europe* EU:C:2009:351.

Case C-495/10 *Centre hospitalier universitaire de Besançon v Thomas Dutrueux and Caisse primaire d'assurance maladie du Jura* EU:C:2011:706.

Joined Cases C-402/07 and C-432/07 *Christopher Sturgeon and Others* EU:C:2009:716.

Case C-128/11 *UsedSoft GmbH v Oracle International Corp.* EU:C:2012:407.

Joined Cases C-503/13 and C-504/13 *Boston Scientific Medizinitechnik GmbH v AOK Sachsen-Anhalt and other* EU:C:2015:148.

Opinions of the Advocate General

Case C-300/95 *Commission of the European Communities v United Kingdom of Great Britain and Northern Ireland* EU:C:1997:255, Opinion of AG Tesauro.

Joined Cases C-503/13 and C-504/13 *Boston Scientific Medizinitechnik GmbH v AOK Sachsen-Anhalt and other* EU:C:2015:148, Opinion AG Bot Y.