CENTRE **I**NTERNATIONAL DE **F**ORMATION **E**UROPEENNE
INSTITUT **E**UROPEEN · **E**UROPEAN **I**NSTITUTE

SCHOOL OF GOVERNMENT

CYBERSECURITY: LIABILITY AND INSURANCE FOR THE INTERNET OF THINGS

BY

Maria Virginia Garcia Romero

A thesis submitted for the Joint Master degree in

Global Economic Governance & Public Affairs (GEGPA)

Academic year
2019 – 2020

July 2020

Supervisor: Lorenzo Pupillo
Reviewer: Benoit Abeloos

Acknowledgements

I would like to express my gratitude to Lorenzo Pupillo for supervising this thesis and for his valuable comments. I am also deeply grateful to Mr. Arnaud Leconte and Mrs. Ana Chokreva-Valette for their generous support throughout this Master.

A special acknowledgment goes to my parents, for their unwavering faith in me.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

AI	Artificial Intelligence
B2B	Business to business
e.g.	For example
EU	European Union
GDPR	General Data Protection Regulation
ID	Identification
i.e.	That is
IoMT	Internet of Medical Things
IoT	Internet of Things
MNC	Multinational Corporation
M2M	Machine to machine
PLD	Product Liability Directive
P2M	People to machine
P2P	People to people
SMEs	Small and Medium Enterprises
WEF	World Economic Forum

Plagiarism statement

I certify that this thesis is my own work, based on my personal study and/or research and that I have acknowledged all material and sources used in its preparation. I further certify that I have not copied or used any ideas or formulations from any book, article or thesis, in printed or electronic form, without specifically mentioning their origin, and that the complete citations are indicated in quotation marks.
I also certify that this assignment/report has not previously been submitted for assessment in any other unit, except where specific permission has been granted from all unit coordinators involved, and that I have not copied in part or whole or otherwise plagiarized the work of other students and/or persons.
In accordance with the law, failure to comply with these regulations makes me liable to prosecution by the disciplinary commission and the courts of the French Republic for university plagiarism.

10 of July, 2020, Maria Virginia Garcia Romero

Introduction

> *"Architecting for longevity and adaptability requires a deep understanding of both today's realities and tomorrow's possibilities. It requires an appreciation for the technology and market forces driving change. And finally, it requires a long-term commitment to focused and incremental progress"* (Deloitte, 2020, p. 5)

Today's reality is that of an era of rapid change, fostered by outstanding technological development. In high-velocity environments, which demand a certain speed in strategic decision-making, one of the biggest challenges policy makers face is '**keeping up**'. For years now, States have been developing, and continue to do so, digital strategies or the so-called "digital agendas" to react and adapt to current circumstances. Although legislation tends to fall behind in these contexts, it is necessary to work exhaustively so that policies address correctly the new societal needs.

Among the technological forces of the 21st century, the **Internet of Things** (IoT). A technology able to transform "*physical objects into smart devices to communicate, as well as interpret, information from the surroundings*" (World Customs Organization, 2019, p. 26). In other words, it "*allows us to monitor and control the physical world remotely*" (Ramos et al., cited in Brous, Janssen and Herder, 2020, p. 1). The IoT has had a disruptive impact in all industries and society as a whole. Its expansion is boosting its economic impact, and its interrelation with other technologies – robotics, biometrics, virtual reality, AI and machine learning, as well as blockchain – has exponentially increased the ways it can be exploited.

The IoT – as well as AI and robotics technologies – has a series of key characteristics: connectivity, autonomy, data dependency, complexity, openness and opacity. Some of these features lead unequivocally to an inherent vulnerability to cybersecurity breaches, since there is a constant interaction with outside information. These cybersecurity breaches can cause systems to malfunction or even trigger the modification of key features causing harm to multiple stakeholders.

Given the benefits and possibilities, but also the associated risks and challenges that new technologies – such as the IoT – bring, more than ever, the political and social discourse

is moving towards safety and security. All over the world, public and private actors are investing in a safer and more stable cyberspace. However, investments in emerging technology require strong regulatory frameworks.

Reports addressing the challenges of new technologies highlight the present need for a clear and somewhat predictable legal framework that covers, among others, liability regulation, in order to ensure that any damage or harm that occurs is remedied efficiently. The underlying issue is not the lack of liability legal frameworks, but its questionable adequacy and lack of clarity. In order to build solid regulatory frameworks, as Deloitte (2020) points out more generally, policy makers must have a deep understanding of today's realities and tomorrow's possibilities technology-wise. There are new actors, new specific and challenging product/service characteristics and more possibilities for cause of damage.

In the European Union, upon interaction with new technologies, there is a persistence to use legal frameworks that could be in part outdated or not completely adequate for the new digital world. Even for the IoT, which is a technology which has been around for some time already, European liability legislation may be falling behind. It is a discussion that started very recently and in 2020 remains open. Hence, one of the research questions lying at the core of this dissertation is whether the EU liability legal framework is adequate and efficient vis-à-vis new technological developments. In addition, if the answer were to be negative, how could liability be allocated adequately and/or efficiently in this legal context?

New opportunities can also emerge when exploring ways to build a safer cyberspace. Although it is not mandatory – policy-wise – certain companies have begun to use insurance policies to mitigate risk associated with cybersecurity breaches. Some experts believe that with the correct set up they could incentivize safer behavior in a more macro scenario. Therefore, this thesis will also aim to discuss cybersecurity in the context of insurance for an emerging digital technology such as the Internet of Things. It will strive to investigate how this element can be used to create better incentives for safer behavior and to work towards convergence between security and safety in the digital sphere.

This dissertation will focus its reach within the European Union (EU), which, wants to lead the transition to a new digital world, grasping all opportunities within safe and ethical

boundaries (European Commission, 2020b). The EU has already emphasized that "*a clear and stable legal framework will stimulate investment, and in combination with research and innovation, will help bring the benefits of these technologies to every business and citizen*" (Commission, 2018, p. 2). The European long-term commitment to the digital sphere and to 'technology that works for people', gives us a chance to delineate new and improved policies for the IoT that can be taken as example for other emerging technologies. But in order to architect for adaptability, questioning and critically assessing what already is in place is of essence.

This thesis will be structured in three main chapters. In Chapter 1, the underlying issue – cybersecurity – will be introduced from a more general perspective, yet with the focus on the emerging technology of the IoT. An overview of the vulnerabilities and associated risks in this context will be provided, considering however, other aspects such as digital trust. In this part, special attention will be dedicated to raising awareness of the cyber challenges faced, as well as enhancing cooperation and collaboration between the multiple stakeholders.

In Chapter 2, the focus will shift towards liability within the European Union. The applicable legal frameworks will be under analysis, pointing out any shortcomings in the system and the underlying reasons. Furthermore, in-depth policy considerations will be presented. Lastly, Chapter 3 will present the idea of using insurance policies in cybersecurity scenarios. Within this chapter, an overview of the market prospects and the challenges faced. The aim is to explore to which extent they can be used to incentivize safer behavior and work towards convergence between security and safety in the digital sphere.

Literature Review

From an academic point of view, cybersecurity studies have been developed frequently over the past years since its introduction to public debate in the mid-1990s. Historically, this field has belonged predominantly to computer sciences and engineering scholars. The literature was very focused on solving the security problem in cyberspace, but also in trying to understand emerging risks in all its facets (Warf, 2018). With the Fourth Industrial Revolution and the speed of technological development, as well as the rising opportunities and risks, research on cybersecurity has grown. In particular, from 2014-2015, with the appearance of sophisticated malware which exemplified the participation of State actors in cyberaggression (*ibid.*). But also, with the introduction of the Industry 4.0 and its related infrastructural vulnerabilities. Such events have lead researchers and policymakers to focus on the relevant issues of safety and security in the cyberspace.

The two research areas of this dissertation – legal liability and use of insurance policies for the IoT – remain a relatively recent theme of research. Accordingly, when carrying on the research, it was necessary to adapt to the limited number of resources. The study is based on material gathered from diverse sources and includes reviews of EU legislation, national frameworks, academic literature, policy papers, EU reports and, civil society and business' reports.

In the first part of the dissertation, the investigation centered on «cybersecurity» from a general perspective, touching upon its prospects and challenges. It heavily relied on reports by the World Economic Forum and Gartner – one of the world's leading research and advisory company. The WEF was especially relevant in terms of analyzing «global risks» and «cyber resilience». Whereas, Gartner provided insights on areas such as the Internet of Things' leverage and security. Articles from experts such as Klaus Schwab – Founder and Executive Chairman of the World Economic Forum – and David Lipton – First Deputy Managing Director of the International Monetary Fund – where also taken into consideration.

In the second part of the dissertation, the work was mainly supported by communications, white papers and reports, written mainly by the European Commission, in the attempt to offer an overview, from official EU legal experts, of the existing liability regimes in the European Union. As well as assess the regimes' adequacy and effectiveness.

Notwithstanding, Chapter 2 was also supported by books sections and academic journals from legal specialists. In the third, and final part of the dissertation, thorough research and review of published literature on «cyber risk» and «cyber insurance» was conducted. These documents include industry reports, academic papers and European Union reports, listed in the Bibliography.

Overall, in this thesis, the intention is to contribute to the debate on the adequacy and effectiveness of liability regulatory frameworks vis-à-vis technological developments. In addition, to propose policy considerations on gaps or shortcomings that are arising. Finally, to explore the role insurance policies and insurers can have in this technological revolution, possibly incentivizing safer behavior and triggering convergence between safety and security.

Chapter 1: Cybersecurity

Cybersecurity has become somewhat of a hot topic. Among the generally accepted definitions, it is defined as the "*preservation of **confidentiality**, **integrity** and **availability** of information in the Cyberspace*" (ISO/IEC, 2012). These elements make up the so-called «CIA triad». Cybersecurity is an approach born to counter the Internet's security problem which started to emerge in public debate around the mid-1990s (Warf, 2018). Ever since, each technological advance has brought new and sometimes unknown **vulnerabilities**.

Yet, why has cybersecurity become critical in order to enable innovation, prosperity and security? The answer is simple enough. Technology has become so deeply interconnected with the economy, our infrastructures and society that its weaknesses are now hazards that can no longer be minimized or ignored. Taking into consideration the IoT, for example, it connects devices and allows remote access. Garnet (2017, p. 5) believes it is a "*foundational capability for the creation of a digital business*" and more than ever enterprises are being built on the foundations of the IoT. However, through its high **interconnectivity** it is amplifying the potential cyberattack surface[1] (WEF, 2020). Cars maliciously controlled remotely, medical devices hacked and controlled for criminal activities, smart homes robbed through hacked intelligent doors, smart watches intercepted while sending sensitive health data to clouds, etc. These no longer are the crimes of the future, but a concrete reality of today. Marc Goodman, founder of the Future Crimes Institute, claims that the challenge with the IoT is that the surface for technological threats is expanding at such exponential rate that "*we have no idea how to defend it effectively*" (Goodman, 2015). If that really is the case, rethinking how to counter harm when it occurs is more than necessary.

It was estimated that by 2020, "*more than 25% of identified attacks in enterprises [would] involve the IoT, although the IoT [would] account for less than 10% of IT security budgets*" (Gartner, 2017, p. 13). The first half of 2019 saw, in fact, an increase in attacks on IoT devices by more than **300%** and the risk of these being used as intermediaries for

[1] In 2017, Gartner estimated there were 21 billion IoT devices worldwide and predicted these numbers would double by 2025.

other attacks is expected to increase (WEF, 2020). Cybersecurity Ventures predicts that by 2021 cybercrime damages might reach **US$6 trillion** (Morgan, 2018).

At stake are: data damage and/or destruction; stolen money; productivity loss; theft of intellectual property or personal and financial data; embezzlement; fraud; post-attack disruption to business as usual, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm (Morgan, 2018). These threats – each day more tangible and dangerous – not only undermine our safety and that of our institutions or businesses, but also our trust in new technologies and the path being undertaken. Yet, there is no stopping the Technological Revolution, it is here to stay, moving fast and without doubt improving people's livelihoods. Somehow this is the price payed for evolution, it is the paradox of progress and it seems that only through effective policy making can people move forward in a sustainable way.

There is certain consensus on the fact that **digital trust** is essential for the IoT – or other technologies – to continue succeeding. Of course, consumers must perceive a certain level of security and privacy in the devices they use, but trust is a very important element able to influence a person's behavior and possibly modify consumption patterns. Nonetheless this is an era of erosion of trust, where among the identified causing factors there is technology[2]. Worries about the future of the job market, the life of established enterprises, the spread of new criminal activities and the so-called weaponization of data deepen said recession (Lipton, 2018). It is essential that the current state of affairs is not underestimated while architecting policies. According to the World Economic Forum, only effective cybersecurity can safeguard such digital trust, spurring "*innovation and progress in society*" and enhancing "*the social responsibility and accountability of organizations*", cumulative effects that enable economic prosperity and inclusion (WEF, no date). Establishing strong legal frameworks which ensure that damages, in case they occur, are remedied and, done so, efficiently could increase the level of trust. A clear set of rules and standards, which allow everyone to know what they attain to, would not only benefit consumers, but the industry in general.

[2] The IMF First Deputy Managing Director David Lipton identifies three factors for trust erosion: the reaction to globalization; the global financial crisis; and technology.

Having witnessed the need for **trust** and **security,** further on it will be observed how they are becoming fundamental pillars of cyber policies. Nevertheless, as already hinted, the interdisciplinary nature of this Technological Revolution and the speed at which it's progressing poses other challenges to policy makers. Since preestablished models, infrastructures and regulatory frameworks are being outpaced, the need – and consequent obligation – for **new tools** to accompany the digital reality is growing. Whether they will be old generation or new one, that is yet to be seen. Most probably it will be a combination of both. Notwithstanding, this arduous task of building cybersecurity frameworks is not just about which tools you use, but about joining forces and involving different actors. This means coming to the realization that humankind faces a common societal challenge that can only be addressed through collaboration and cooperation. A notion that, although it may seem straightforward, has multiple difficulties that will later be discussed.

1.1. The paradox of progress

The Forth Industrial Revolution evolves at an exponential pace, combining technologies that are bringing forward unprecedented paradigm changes in our society, economies and politics. This digital world that is being built is powered by big data, artificial intelligence (AI), the Internet of Things (IoT), 5G networks and cloud storage, among many other technological advances. As Klaus Schwab put it, "*there has never been a time of greater promise, or one of greater potential peril*" (Schwab, 2016).

On the one hand, the innumerable benefits for public and private actors, as well as for individuals are self-evident and self-explanatory. Communications have become faster and more reliable, enhancing commerce and enabling telecommuting and teleworking. Technology has made the world more efficient and productive, employing smart administration, reducing paperwork, improving processes and interconnecting operations. The reduction in bureaucracy should lead to greater transparency and better accessibility. Overall it has led to cost reduction in multiple sectors, which has contemporaneously translated into an increase in profits in businesses worldwide.

Currently, "*digital technologies have become the backbone of our economy and are a critical resource all economic sectors rely on. They underpin the complex systems which keep our economies running*" (European Commission, 2017, p. 1). Their deep integration in every aspect of our life and the essential role they play in our society, make them a

target and a global risk. Growing cybersecurity threats, including but not limited to cyber espionage, cyberwarfare and cybercrime, have an enormous **power of disruption**.

Cyberthreats are in constant evolution and they take advantage of online behavior and new trends or opportunities. One of the biggest trends is the lack of basic computer hygiene and that businesses, more often than not, react rather than prepare for cyberattacks (Pupillo, 2018). Some of the biggest corporate or institutional hacks of all times, ranging from the exposure of a few million records to several billion, have monopolized the news and worried citizens worldwide. Cybercriminals target governments and industries, although technology companies, retail and financial institutions are the most affected (Kammel, Pogkas and Benhamou, 2019). To remember some of the most prominent: the attacks on the European Parliament, Commission and the EU's Emissions Trading Scheme in March 2011; the Yahoo hack of 2013[3]; JP Morgan Chase attack in June 2014[4]; UniCredit hack in 2015[5]; MyFitnessPal in February 2018[6]; Facebook in September 2018[7]; the hack on the Indian government ID database, Aadhaar, in 2018[8]. The information accessed in hacks can be used to engage in all kinds of fraud, since even if it is not sensitive in itself, it is frequently used to validate people's identities. Another recent trend has been the 'cyber-intervention' in elections worldwide. One of the most emblematic cases was the 2016 American elections.

Currently, cybercriminals are exploiting the Coronavirus pandemic – since cyber defenses may be lower because of the health crisis – to: develop highly dangerous malware campaigns; register malicious domains; spread fake covid19 news; and to target hospitals, medical centers and public institutions for ransomware attacks (Interpol, 2020).

[3] Over 3 billion accounts were compromised. It was reported to be the biggest known breach of a company's computer network (Perlroth, 2017).
[4] 83 million records of households (76 million) and small business (7 million) accounts were compromised. They included names, addresses, phone numbers and email addresses (Agrawal *et al.*, 2014). The US federal indictments in the case in 2015 mention that the email addresses were later used in "pump-and-dump" schemes to boost stock prices. For more information see (Pagliery, 2015).
[5] Almost 3 million Italian records were accessed. They included names, cities, phone numbers and emails (Repubblica, 2019).
[6] About 150 million users' personal data was hacked. Among the stolen data: user names, email addresses and scrambled passwords (The Guardian, 2018).
[7] The breach exposed the personal data of 29 million users. The attackers took birth dates, employment and education history, religious preference, types of devices used, pages followed, recent searches and locations (Vengattil and Dave, 2018).
[8] Over 1.1 billion records of registered citizens were compromised. Access to the database was later sold by cybercriminals.

The Global Risks Report 2019 published by the World Economic Forum (2019), ranks 'massive data fraud and theft' as number four global risk by likelihood over a 10-year horizon, and 'cyber-attacks', at number five. As highlighted, "*the vulnerability of critical technological infrastructure is a growing national security concern*" (*ibid.*, p. 23).

These events unveil the so-called **paradox of progress**, "*our society is more efficient as digitalization progresses, but it is also more fragile*" (Pupillo, 2018, p. 1). Wealth was created, efficiency increased and more convenience in technological solutions was found, hence all that could be connected was connected (Shull, 2019). Such connectivity, digitizing society, translated into "*building inherent vulnerability into the core of the economic model*" (*ibid.*, p. 4). Notwithstanding, this all implies that, "*the same trends generating near-term risks also can create opportunities for better outcomes over the long term*" (US National Intelligence Council, 2017, p. 9). It is time to build cyber-resilience so that public or private actors will be able to exploit those opportunities, while adapting to new circumstances, persevering in case of unexpected adversity and adopting strategies for quick recoveries (*ibid.*).

1.2. A Common Societal Challenge

In our digital scenario, cyber breaches, data misuse cases, election-meddling, etc. are almost too familiar news. As mentioned earlier anyone can be a target, no difference being public or private sector. It has been highlighted that users no longer feel they have any control over what happens with their personal data (European Commission, 2020b). Often because data breached incidents come to light only time after they have happened. Therefore, even if you have been hacked, you may not ever know.

Cybersecurity unfolds as a **common societal challenge**. Cyberattacks have the potential to be destructive, threatening our personal well-being, and disruptive to sensitive infrastructures and communication systems. Since it is a shared issue, it should become somewhat of a collective responsibility, pushing everyone to work together. For this reason, certain types of collaboration or cooperation are in order.

In this line, citizens should be witnessing constant and strong **collaboration** and compromise between **public and private spheres**, working together to strengthen such systems and infrastructures. Because there is a need to open the dialogue – both technical

and ethical – across the multiple disciplines and stakeholders. Yet, collaboration between public and private sectors is, to say the least, difficult. The underlying reasons are varied. Both play complex roles in society, with different responsibilities and obligations "*vis-à-vis each other and the citizens who rely on them*" (WEF and Boston Consulting Group, 2017, p. 5). Furthermore, security, is an area "*deeply connected to notions of sovereignty*", thus MNCs and customers may come across "*contradictory national obligations*" (*ibid.*). Besides, in the context of cybersecurity, the situation is exacerbated because by combining security with other values (e.g. people's private lives) "*the need to be inclusive in representing and negotiating between different interests and principles*" is magnified (*ibid.*). Whatever the difficulties, there are already leaders in both spheres attempting to begin framing the discussion and putting the focus on five key values: security, privacy, economic value, accountability and fairness (WEF and Boston Consulting Group, 2018).

At the same time, there is need for a different type of collaboration: **multilateral**. The World Economic Forum (2020, p. 62) emphasizes that "*the lack of a global governance framework for technology risks fragmenting cyberspace, which could deter economic growth, aggravate geopolitical rivalries and widen divisions within societies*". Our context, however, is that of a shift from multilateralist to unilateralist tendencies, as well as of stepping up competition rather than cooperating. Since innovation translates into power – economic, military, geopolitical, etc. – the world's leading powers rush to invest heavily in emerging technologies to secure a place as influencers. But when it comes to regulation, global consensus faces a challenge and incentives are low. The risk is ending up with a "*global system wherein the incentives align with the creation and spread of new technologies […] but not with the oversight of them*" (Engelke, 2018). This empowers technology yes, to a certain extent, but also increases the risks to be faced.

Although States may not be ready to negotiate international regulation on emerging technologies, opening the discussion at a global level can have beneficial effects on governance (Engelke, 2018). Participation in multilateral forums can help States in the elaboration of standards and rules on thorny subject areas which they will be forced to regulate at a national level eventually. Regional cooperation, exemplified by the European Union, are also important steps forward in terms of cybergovernance.

In spite of the previous considerations on collaboration – whether multilateral or between public and private sectors – it is also true that, in terms of cybersecurity, **individuals** have a big role to play. More often than not, they are described as "*the **weakest link** in the security chain because they often fail to comply with security best practices*" (Donalds and Osei-Bryson, 2020, p. 1). Not surprisingly, over 90% of "*successful hacks and data breaches stem from phishing, emails crafted to lure their recipients to click a link, open a document or forward information to someone they shouldn't*" (Morgan, 2018). Cybersecurity experts agree that even if companies put in place layers upon layers of security, if people are unaware of cyber-threats and the ways to detect and report them correctly, these measures are then rendered futile (*ibid.*). What emerges is the importance of digital literacy training, not just circumscribed to companies but presented as part of a more far-reaching program. In this way, cyber awareness could be enhanced across different audiences, while basic computer hygiene could become part of people's everyday habits.

Overall, it is essential to raise awareness, not only political but also societal, because cybersecurity is a challenge that can only be faced collectively. Becoming responsible begins from individuals and slowly escalates to involve more and more stakeholders until a whole culture around cybersecurity is built.

Chapter 2: Liability for the Internet of Things (IoT)

The overall aim of a liability regime is to 'repair' or 'remedy'. That is, to either try to reestablish a situation before the production of a damage that shouldn't have been endured or to compensate the victim for the harm suffered. Strong liability frameworks protect consumers, incentivizing wrongdoers to avoid causing damage again. Contemporaneously they build trust in new technologies – an essential element for their take off. They do so by striking a balance between citizen protection and enablement of business innovation (European Commission, 2020a).

In this Chapter some of the questions most recently raised at EU level will be discussed. In particular, analyzing liability regimes, identifying gaps and looking for ways to strengthen them. Their adequateness and completeness as new technologies, such as the IoT advance, are of essence, otherwise deficiencies may result in victims being totally or partially uncompensated.

The following sections will explore the current legal framework at EU and national level, as well as the changes in the environment and challenges faced. All this without losing track of the research questions at the core of this dissertation – is the EU liability legal framework adequate and efficient vis-à-vis new technological developments? And, if the answer were to be negative, how could liability be allocated adequately and/or efficiently in this legal context?

2.1. Introductory concepts

Liability is a legal concept closely linked to that of obligations and responsibility. It has been defined as the "*responsibility of one party for harm or damage caused to another party, which may be a cause for compensation, financially or otherwise, by the former to the latter*" (European Commission, 2018b). An existing legal relationship between the parties – i.e. a concrete obligation – may be its origin, but also the violation of a legitimate interest or right. These notions cover some of the more traditional concepts of **contractual** or **non-contractual (tort) liability**. A situation may fall under one of the two categories depending on whether the law requires that there is **fault** or not in the author's conduct when the victim demands compensation. In order to have a legal basis

supporting a compensation claim, three essential elements generally must be present as prerequisites: damage, causal link and misconduct[9].

The **damage** may consist in an economic loss, also known in certain systems as 'patrimonial or material loss'. It refers to when the undermining of the victim's interests can be valued in money, for example, the damage to property. On the other hand, the damage may also consist in a non-economic loss or 'non-material damage'. That is a loss that cannot be easily quantified monetarily. These could comprehend moral damages such as pain, suffering, emotional distress, etc. As can be seen, the concept of damage is quite flexible given that the range of interests under legal protection can vary greatly, some being more significant than others. However, it must be noted, that throughout Europe what may be considered compensable harm is not harmonized and depends on the national legal regime applied. Indeed, in the case of data damage or destruction, there is not yet consensus across Europe on whether this is property loss (Expert Group on Liability and New Technologies, 2019). Why? Because property, as a legal concept in certain jurisdictions, is circumscribed to corporeal objects, with the exclusion of intangibles (*ibid.*). Although this may be true, article 82 of the General Data Protection Regulation, harmonizes the right to compensation and liability in cases of data releases which infringe the right to privacy.

The **causal link** or **causation** is another essential prerequisite for a declaration of liability to occur. It's the relation between what caused the damage and the damage *per se* (cause-effect). Nonetheless, although it must be present for contractual or non-contractual liability, certain legal systems such as the Spanish, break the causation in special circumstances such us: fortuitous events or force majeure; actions belonging to a third party; or actions from the victim (Wolters Kluwer, no date).

Whatever the exceptions may be, the fact is that the causal link must be **proved**. Normally, the burden of proof lies on the victim, something that with emerging technologies may give place to complex situations. In such contexts, being able to determine the exact chain of events is often difficult. Especially when multiple factors may have contributed to the final damage and when algorithms or self-learning technologies may be involved. By itself, the mere tracking of the origin of the damage is

[9] This last prerequisite depending on the type of liability applied.

a challenge but adding to it the financial costs required for the analysis by an expert poses further obstacles for victims to attempt liability claims in this field (Expert Group on Liability and New Technologies, 2019). Under certain circumstances (mostly strict liability cases) the **burden of proof is reversed**, since the legislator believes the general rule to be too burdensome for the victim. Here, instead of establishing the casual link, what must be proved is that the "*risk triggering strict liability materialized*" – this risk then being properly defined by each system (*ibid.*, p. 21).

Notwithstanding the burden of proof – which is quite a relevant factor to consider for the parties involved – the issue of **uncertain causation**, upon which compensation also depends, is being addressed within the European Union. Currently European legal systems handle uncertainties or alternative causation differently. It may be that "*no-one is liable (since the victim's evidence fails to reach the threshold to prove causation of one cause), or that all parties are jointly and severally liable, which is the majority view*" (Expert Group on Liability and New Technologies, 2019, p. 22). Some modifications are being applied so that, given specific cases, the victim's burden of proof is alleviated, yet not reversed (*ibid.*, p. 21). For instance, accepting *prima facie*[10] evidence in more complex scenarios. The positive future repercussions of these modifications or updates in legislation mustn't be overlooked, especially given the characteristics of emerging technologies: interconnectedness, data dependency, openness, etc. Indeed, it will become increasingly problematic to determine whether a damage was triggered by a "*single original cause or by the interplay of multiple (actual or potential) causes*" (*ibid.*, p. 22), so these measures could be very beneficial.

The third prerequisite is not homogenous in all liability regimes and it consists in a conduct that causes someone to suffer a damage. Ranging from actions to omissions, fault to negligence or even the infringement of the duties of care, many may be the configuring elements that can help courts assess whether someone has deviated from what was reasonably expected. Across Europe there is a tremendous level of confusion and misunderstanding when it comes to referring to these conducts. Depending on the applicable legal system it may be known as **fault**, **wrongful behavior** (also *wrongfulness*)

[10] Prima facie means that it is "sufficient to establish a fact or raise a presumption unless disproved or rebutted" – Cornell Law School, Legal Information Institute. For more information see: https://www.law.cornell.edu/wex/prima_facie

or as a combination of both. To be clear, these terms usually do not mean the same thing. Yet, to prove the confusion, a more practical example. In certain legislations wrongful behavior is determined objectively, since it is considered to be a conduct that has violated the law, harmed an interest protected by it, or has a harmful status that is against the law (Elischer, 2017). Given these circumstances it is not hard to guess that fault is seen as a subjective element. Regardless, in France, Poland, Hungary and England, fault is assessed objectively, sometimes even having difficulties distinguishing it from wrongfulness (Koziol, 2015). As a result, the terms bear a blurry relationship, highly dependent on jurisdiction, but disorienting at a macro EU level.

When discussing technologies such as the IoT, which are usually integrated with AI applications creating complex systems, it is difficult to apply fault-based liability rules. As was pointed out earlier, in combining different components, it becomes more challenging to pinpoint the origin of a potential damage, but also to determine **who** is to be found liable since the number of actors involved increases (European Commission, 2020a). At the same time another issue arises: legislation regulates duties of care for human conduct, but there is nothing for technologies learning without direct human control (Expert Group on Liability and New Technologies, 2019). The new features now empowering the IoT and AI will eventually require regulation, even if at a minimum level. By defining requirements, any violations could "*trigger liability more easily for the victim*" (*ibid.*, p. 23).

To summarize, in liability claims within the European Union, two to three prerequisites must be met: the damage, the causal link and the wrongful behavior or fault depending on the type of liability. From a preliminary analysis emerges that litigation for victims – in cases where emerging technologies such as the IoT are involved – may be burdensome, time-consuming and expensive.

2.2. Overview of existing liability regimes in the European Union

Liability regulation at EU level is interlinked with product safety frameworks. The overall aim is to provide trust and safety to all consumers (European Commission, 2018b). When exploring liability rules applicable in the context of emerging digital technologies within the European Union, there is a reliance on the parallel application between EU law and national law (European Commission, 2020a).

2.2.1. EU level

At the present time, the Product Liability Directive of 1985[11] positions itself as one of the most important examples of EU liability harmonization. Other than this exists liability for violation of data protection law[12] or competition law[13], a regime relating to insurance against civil liability resulting from using motor vehicles[14] and a framework for solving conflict of tort laws known as Rome II Regulation[15]. Excluding these exceptions, the rest, is mostly non-harmonized and dependent on national legislation.

The Product Liability Directive (from now on the 'Directive' or 'PLD'), was born to counter the legal divergencies among Member States regarding the liability of the producer for damage caused by the **defectiveness** of his products. At the time, it was believed that such differences could in some way distort competition, affect the free movement of goods in the common market and provoke various degrees of consumer protection. Therefore, the European Communities codified a short liability regime – to complement the national frameworks – which was without fault, what is known as a **strict liability regime**. For the legislators it was the "*sole means of adequately solving the problem, peculiar to our age of increasing technicality, of a fair apportionment of the risks inherent in modern technological production*" (Council Directive 85/374/EEC, preamble). The underlying rationale of this Directive was that the " *threat of monetary damages stemming from legal actions [would] incentivize actors to implement the necessary measures to minimize the risk of failures or defects*" (Studer and De Werra, 2017, p.514). As a result, in this context the victim no longer must prove a fault of the producer, but instead is required to prove (burden of proof) the damage, the defect and the causal relationship between defect and damage (article 4 of the Directive).

[11] 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.
[12] The previously mentioned article 82 of the General Data Protection Regulation (GDPR).
[13] Directive 2014/104/EU of the European Parliament and of the Council of 26 November 2014 on certain rules governing actions for damages under national law for infringements of the competition law provisions of the Member States and of the European Union.
[14] Directive 2009/ 103/ EC of the European Parliament and of the Council of 16 September 2009 relating to insurance against civil liability in respect of the use of motor vehicles, and the enforcement of the obligation to insure against such liability.
[15] Regulation (EC) No 864/ 2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II).

Definitions of what a product is or who can be considered a producer are provided by the Directive, bringing legal clarity across the Union. A producer is "*the manufacturer of a finished product, the producer of any raw material or the manufacturer of a component part and any person who, by putting his name, trademark or other distinguishing feature on the product presents himself as its producer*" (Article 3). Whereas products are all **movable** objects, mostly tangible, but including electricity (Article 2). The Court of Justice stated that products used while providing services are still under the range of application of the Directive, yet that this is not the case for the liability of a service provider (European Commission, 2018b).

The framework is known to be «**technology neutral**», a principle representing the "*freedom of individuals and organizations to choose the most appropriate and suitable technology for their needs*" (European Commission, 2019). In the case of the Directive, it means that the liability regime presented does "*neither impose nor discriminate in favor of the use of a particular type of technology*" (*ibid.*). It is an important element to note because it is what has kept the legal framework relevant over the years.

As stated earlier, questions have arisen on the **effectiveness** of the current legal liability frameworks **vis-à-vis** the spread of **new technological developments**. For this, as well as other reasons, the Product Liability Directive was evaluated in 2018 by the European Commission. A series of consultation activities were also launched to the general public for better assessment and the results were quite interesting. "*45% of producers, 58% of consumers and 44% of the other respondents (including public authorities/ civil society) consider that for some products the application of the Directive might be problematic or uncertain […] due to their complexity and degree of automation"* (European Commission, 2018a, p. 33). The products mentioned were software/applications belonging to different sources that could be installed post purchase, products performing automated tasks (algorithm-based), data analytics, self-learning algorithms or products purchased as a bundle with related services (*ibid.*). What was identified as an issue, with the potential to challenge the framework as a whole, were some of the features of new technologies (*ibid.*). Autonomy, which comes with algorithms and self-learning capabilities, and complexity, which adds more components but also more actors, both reduce the level of **control** the producer has over the product. This, in terms of liability, has a tremendous impact. **Who** then should be held liable if something goes wrong?

Contemporaneously, there are repercussions at a purely terminological level. The Directive is circumscribed to products and they are defined, but now more than ever the line between product and service is blurred (Expert Group on Liability and New Technologies, 2019). Software, for example, is now built-into the product but it can also be supplied separately to allow the product's use. Is it covered by the Directive? It isn't clear. The software could eventually render a product defective and cause a damage. These scenarios require special attention from a safety perspective but also from a liability one. All in all, the scope of the Directive should be clarified given the new circumstances (European Commission, 2018a, p. 61). Similarly, the definition of producer needs to be updated, even more as products and services are combined (*ibid.*).

Another important element in the Directive is the notion of **defect**. The basis for its assessment is the safety which a consumer is entitled to expect, all relevant circumstances considered (Article 6, paragraph 1). As was introduced when discussing the causal link, identifying the origin of a defect can be troublesome when dealing with emerging technologies. If the IoT devices are involved, the interconnectedness of the multiple systems, software and maybe even integrated AI technology render proving the defect and causation burdensome. The presence of "*AI autonomous systems with self-learning capabilities also raise the question of whether unpredictable deviations in the decision-making path can be treated as defects*" (Expert Group on Liability and New Technologies, 2019, p. 28). Given the slight possibility they could be treated as defects, producers could use one of the exceptions of Article 7 to not be held liable – known as «state-of-the-art defense[16]» or «development risk defense». Consequently, consumers could lose certain level of protection.

Although the consultation activities found that, producers and insurers didn't feel the need to update the Directive from a business to business (B2B) liability perspective, they did acknowledge that difficulties could arise for business to consumer (B2C) relations in the future. In this line, most consumers maintained that the Directive needed to be updated for the new technological developments. Some of the main arguments business associations used against revising the existing framework were that it was technology

[16] This is exception is recognized in article 7 (e) of the Directive: "The producer shall not be liable as a result of this Directive if he proves […] 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".

neutral, fit for its purpose and – time-wise being – still premature to alter regulation (European Commission, 2018a). An issue brought up was the lack of "*concrete evidence of real-life problems*" and experience with damages caused by new technological developments at the time. Yet, something that can be, at the very least, put in question is whether it can be reasonable to expect a substantial number of cases of compensation claims for damages produced by emerging new technologies. Particularly, in a scenario of increased complexity and interconnectedness, with new actors, no regulatory updates, heavy expenses and no certainty of the outcome. Whatever the situation may be, Member States have stated that they prefer to collect "*robust evidence of shortcomings before amending the current legal framework*" (*ibid.*, p. 35).

All things considered, the effectiveness or ineffectiveness of the Directive vis-à-vis technological developments could not be definitively concluded by the European Commission in 2018, remaining a contested subject. What was generally agreed upon, mainly by public authorities, civil society and consumer associations (not businesses), was that the issue of technological developments was **not adequately covered** by the Directive.

2.2.2. Member State level

In Member States, EU liability legislation coexists with national frameworks. Therefore, the presence of the Product Liability Directive does not preclude the use of other regimes that may exist in the country. For example, contractual or non-contractual liability based on different grounds of those allowed by the Directive.

Generally speaking, it has recently been observed that, on a Member State level, legal frameworks "*[do] not (yet) contain liability rules **specifically applicable** to damage resulting from the use of emerging digital technologies*" (Expert Group on Liability and New Technologies, 2019, p. 15). The exceptions discovered are in the area of automated vehicles (*ibid.*). Jurisdictions allowing either the experimental or regular use of these vehicles are the ones taking the first steps regulation-wise. It is interesting to note that

these Member States[17] started by establishing the obligation to have **insurance** providing coverage for any damage caused.

Attempting to cover all the different types of more traditional liability that may be present in a Member State would be notably difficult and escape the scope of the dissertation. For this reason, this section will only cover the more relevant categories that could be applicable in the context of emerging digital technologies: fault-based non-contractual liability, strict liability and vicarious liability.

Within non-contractual liability regimes (or sometimes known as extra-contractual), **fault-based liability** can be found. In this category the focus is on the *fault* of the author of the misconduct that led to the damage. As was introduced in the above section, the wrongful behavior could have been an act or an omission, but in this case, it could have been intentional or out of negligence. For the claim to succeed, the fault must be proven, something which normally the victim has to do (European Commission, 2018b). However, some exceptions exist to make it less burdensome, especially under circumstances of imbalance of information between the parties. In occasions, the presumption of fault lies by the wrongdoer – the reversal of the burden of proof – unless he proves he is not to be held liable (*ibid.*).

Other legal frameworks may contain **strict liability**. It is still a type of extra-contractual liability, but irrespective of fault. That is, the prerequisites for a compensation claim are only two, the existence of damage and the causal link. Behind the legislator's rationale is the thought that, in certain situations, applying the general fault-based liability rule is too burdensome or unbalanced (European Commission, 2018b). The scenarios under consideration are varied but always connected to the materialization of the **risk of damage** and circumstances that **cannot be avoided** or foreseen (*ibid.*). In some cases, it can be linked to the unpredictable behavior of specific risk groups – animals or persons –

[17] In particular, references are made to: Italy – Article 19 of the Italian Decree of 28 February 2018 on the testing of connected and automated vehicles on public roads (Modalità attuative e strumenti operativi della sperimentazione su strada delle soluzioni di Smart Road e di guida connessa e automatica, 18A02619, GU n° 90 of 18 April 2018) – Spain – Directorate-General for Traffic (Dirección General de Tráfico) circular of 13 November 2015 (Instrucción 15/V-113) – Germany – § 7 of the German Road Traffic Act (Straßenverkehrsgesetz) – and France – French Decree n° 2018-211 of 28 March 2018 on experimentation with automated vehicles on public roads relies on the Loi Badinter of 5 July 1985 (n°85-677). All examples mentioned by the Expert Group on Liability and New Technologies (2019).

whereas, other times to certain activities – transportation[18], energy[19] or pipelines. As can be noted, the relevance of this category lies in its wide range of application.

Strict liability was introduced by legislators from the 19th century onwards, to counter the "*risks brought about by new technologies*" (Expert Group on Liability and New Technologies, 2019, p. 25). Currently, there is strict liability legislation for motor vehicles (in some Member States) or aircrafts that could be applicable to autonomous vehicles or drones (*ibid.*). However, the Expert Group on Liability and New Technologies (2019) has highlighted the many potential liability gaps. In the area of operation of computers and/or software, the Expert Group has only detected a limited number of Member States "*providing for the liability of the operator of some computer system, such as databases operated by the state*" (p. 26).

Vicarious liability, on the other hand, is a type of liability contained in many legal regimes. It is an extra-contractual responsibility attributed to someone – the principal – for the wrongful behavior of another – the auxiliary. For this reason, it is often known as the «**liability of others**». Approaches vary across jurisdictions when it comes to the specific circumstances or prerequisites upon which the principal is held liable. Regardless, this concept "*is considered by some as a possible* ***catalyst*** *for arguing that operators of machines, computers, robots or similar technologies should also be strictly liable for their operations, based on an* ***analogy***[20] *to the basis of vicarious liability*" (Expert Group on Liability and New Technologies, 2019, p. 25). This risk exists because legislators are not defining nor regulating the new concepts, actors or relations. Therefore, if damages occur victims will have to turn to the available legislation and, among it, they could attempt a case of an analogical application of vicarious liability for operators of machines, etc. Nevertheless, if that were to be accepted, the challenge would then lie in identifying the "*benchmark against which the operations of non-human helpers will be assessed in order to mirror the misconduct element of human auxiliaries*" (*ibid.*).

To conclude, national liability frameworks do not contain – apart from a few exceptions – **rules specifically designed** to adequately solve damage claims resulting from the use

[18] For example, damages originating from driving a car or piloting an aircraft.
[19] For example, operating a nuclear plant.
[20] Analogy is tool used to close normative gaps. Within each legal order, the use of analogical reasoning has a specific impact and importance.

of emerging digital technologies. The general trend observed is to continue using traditional regimes, both European and national, and resort to legal analogy when necessary. Although these frameworks may still be efficient and relevant, the existing gaps contest its adequateness.

2.3. IoT characteristics and other regulatory challenges faced

The Internet of Things portrays many of the features that emerging digital technologies have, i.e. complexity, autonomous behavior, data-drivenness, vulnerability and openness. These characteristics challenge the current liability framework in ways already touched upon and others yet to be discussed. However, to understand truly the policy issues posed, it is necessary to give an overview of how the technology works.

To begin with, the IoT has a far-reaching potential. Its vision has been defined in the following terms:

> Internet of Things heralds the vison of such a paradigm which connects virtual or physical objects (Anything) and people of any age group (Anyone) through wired or wireless connections (Any network) in order to benefit the consumers (Any service) who are positioned anywhere (Any place) without the involvement of time constraints (Any time) (Khan *et al.*, 2016, p. 112).

From this definition three major agents emerge as key aspects of the IoT – **people**, **objects** and **data**. The connections that are facilitated are of course people to people (P2P), but also machine to machine (M2M) and people to machines (P2M) (*ibid.*).

The IoT is made up of various technologies such as sensors or embedded systems. One of the issues that emerges is that sensors can be publicly accessible, and any weak link can be easily exploited by cyber-criminals (*ibid.*, p. 113). This **vulnerability** is part of one of its main features: **openness**. Since systems need to interact among each other or with data sources, they need to remain open by design[21] (Expert Group on Liability

[21] As the Expert Group on Liability and New Technology (op. cit.) explains, these technologies new to allow "external input either via some hardware plug or through some wireless connection".

and New Technologies, 2019). The frequent updates or upgrades they undergo are also a major source of weaknesses that enable cybersecurity breaches.

Despite the above, when sensors are connected – either in private, business or city environments – they collect data from objects. For this reason, another of its features is «**data-drivenness**». The Internet of Things is dependent on data – external information gathered or communicated – to function properly. This data though, can be flawed or missing because of "*communication errors or problems of the external data source*" (European Commission, 2018b, p. 33). Once collected, the information is analyzed through "*embedded systems or through cloud-based and Internet systems, enabling the creation of new services based on big data analytics*" (*ibid.*, p. 22). It is important to mention that data provided through an IoT ecosystem is considered as a service, which means that the product liability and safety regimes cannot be applied (European Commission, 2016, p. 22).

Thanks to the data gathered, IoT devices can take decisions and perform specific functions (European Commission, 2018b, p. 33). This ability is known as «autonomy» or «autonomous behavior» - "*being able to perform tasks with less, or entirely without, human control or supervision*" (Expert Group on Liability and New Technologies, 2019, p. 33). Autonomous behavior, as has already been mentioned, raises legal questions because it is capable of modifying a product's key characteristics (e.g. its safety). Can these self-learning features extend the liability of the producer? And in the same line, can the producer really foresee all the changes that this technology can produce? In reality, autonomous IoT devices have a potential to cause harm, which consequently poses risks to liability.

At the same time, this technology with all its components, also "*becomes part of a bigger connectivity network*" creating "*new opportunities to combine more intelligence and actuation across vertical markets and to provide a whole new set of services*" (*ibid.*). Overall, what the IoT does is set up **ecosystems** that have a cross-cutting effect on vertical areas, creating "*new markets for hardware (connected devices), software (IoT platforms and systems) and services (IoT applications)*" (European Commission, 2018b, p.22). Here lies its **complexity**, in its heterogeneity and interoperability. The IoT ecosystem is

heterogenous in nature – it is the result of the integration of multiple objects[22], that belong to different manufacturers and that have different functions (Khan *et al.*, 2016). By bringing together a wide range of actors[23] from diverse sectors, the value chain is rendered increasingly complex (*ibid.*). Consequently, such level of complexity leads to more **opacity** for those benefiting from their functions (Expert Group on Liability and New Technologies, 2019). That is, it is difficult to understand how the technology is working or what may be a possible cause of harm. From a liability perspective, identifying who – among the multiple stakeholders – is to be held liable is challenging and burdensome. In the same line, other questions emerge: "*who is responsible for guaranteeing the safety of a product? Who is responsible for ensuring safety on an on-going basis? How should liabilities be allocated in the event that the technology behaves in an unsafe way, causing damage?*" (European Commission, 2016, p. 22).

When it comes to further discussing the regulatory challenges faced, one evident mention emerges: cyber-attacks. Allocating liability in such scenarios is difficult because assessing a company's legal exposure after a cyber-attack poses more questions than answers. Of course, the cyber-criminal is liable, but usually the attacks are anonymous so attempting a compensation claim against the attacker would be close to impossible. Therefore, the debate centers mainly around businesses and legal concepts such as «**due care**» and what level of cybersecurity can be deemed "*reasonable and appropriate so that, notwithstanding an attack, no liability can be assigned to the victim*" (Studer and De Werra, 2017, p. 512). But then again, what are reasonable cybersecurity measures? In order to answer, standards must be developed. Only then can courts effectively contrast the measures with the standards, taking into account the context and the damage produced. Yet other questions arise. Can liability be imposed in situations of potential secondary liability? (*ibid.*) In addition, a recurrent question, when multiple actors are involved in a cyber-attack (voluntarily or not), if there is liability at all, how to allocate it among the different parties?

If a contract is in place, contractual liability applies. Theoretically a user could file a complaint "*on the basis of a contractual promise of security, contained for instance in a*

[22] i.e. It integrates physical objects, software, Internet infrastructure, the behavior of the final user, etc.
[23] e.g. Product manufacturers, sensor manufacturers, software producers, infrastructure providers, data analytics companies and other actors that supply different services, as well as final users.

privacy policy" (Studer and De Werra, 2017, p. 512). However, its practical implementation is questionable. Businesses usually don't include in their terms of service any promise of (cyber) security resilience (European Commission, 2018b). The usual praxis is to include, in the terms of service, warranty disclaimers and limitations of liability to minimize or exclude any civil liability (*ibid.*). Unless the vendor was **grossly negligent** in the implementation and maintenance of adequate cybersecurity measures – in which case the liability limitations would be considered null and void – the risks of holding him liable for a cyber-attack seem to be low.

If no contract were to be in place, non-contractual or tort liability could be applicable. This is valid for cases of cyber-attacks in which third parties suffered harm. In the European Union, different legal frameworks could be used to ascertain liability, such as the **General Data Protection Regulation** and the **Product Liability Directive** mentioned above.

Since May 25, 2018[24], companies have had to comply with the GDPR, known as "*the toughest privacy and security law in the world*" (Wolford, no date). This regulation is far-reaching, extending its range of action to all businesses, irrespective of their location, as long as they "*target or collect data related to people in the EU*" (*ibid.*). Non-compliance is harshly fined with penalties that can reach tens of millions of euros or even a percentage of the total worldwide annual turnover of the preceding financial year[25]. As was discussed the GDPR includes a civil liability regime in article 82 for data controllers or processors[26]. Ex article 82.2, data controllers are liable for the damage caused by processing which infringes the Regulation. Whereas processors are liable for the damage caused by processing only where it has not complied with obligations of the Regulation specifically directed to processors or where they have acted outside or contrary to lawful instructions of the controller (art. 82.2).

[24] Date in which the regulation was put into effect.
[25] Article 83 GDPR.
[26] According to Article 4, paragraph (7), a controller is "*the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data*". Whereas a processor, ex Art. 4, paragraph (8), is "*a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*".

The obligation established by the GDPR is that of means. In fact, article 32.1 states:

> Taking into account the **state of the art**, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement **appropriate technical and organisational measures** to **ensure a level of security appropriate to the risk**… (Regulation 2016/679, 2016).

Among the relevant aspects of this provision, the «state of the art» clause and the "appropriate measures" that must be taken to ensure an "appropriate level of security".

The «state of the art» clause is an exception present in many regulations, for example the Product Liability Directive. In the same line, it excludes liability in cases of products that do not ensure safety "*if the producer demonstrates that the state of scientific and technical knowledge at the time when it put the product into circulation was insufficient as to enable the existence of the defect to be discovered*" (Machnikowski, 2016, p. 695). Its relevance lies in the fact that the existence of liability is tied to "*a decision taken at the time the product was put on the market, exclusively on the basis of available data and opinions on the adequate level of product safety*" (*ibid.*). In a cyber-attack scenario, a manufacturer could use this clause to allege that when the product was placed on the market no software vulnerability was discovered.

In that which regards the appropriate measures that must be taken, these aren't specified, though some examples are offered in paragraphs a) to d):

> (a) pseudonymisation and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing (Regulation 2016/679, 2016).

The mention of «an appropriate level of security» is further delineated in the second paragraph of article 32. According to it, the "*risks that are presented by processing, in*

particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed" must be considered when assessing if the level of security was appropriate.

Overall, the liability regime provided by the GDPR is that of strict liability, that is irrespective of fault. Controllers and processors will be exempt of liability only if they prove that they are not responsible for the event that triggered the damage "*in any way*" (Article 82.3 GDPR). The practical meaning of "in any way" remains unclear, however, it "*seems to indicate a willingness to narrow the scope of the liability exemption*" (Studer and De Werra, 2017, p. 513).

As was earlier mentioned, the Product Liability Directive also establishes a strict liability regime. Nevertheless, liability is circumscribed to the producer, excluding third parties. In the IoT context, challenges emerge. Some questions have been raised in terms of how to "*determine what the product liability exposure of software vendors to claims for personal injury and property damage caused to third parties could be*" (Studer and De Werra, 2017, p. 514). In the same line, the interpretation of 'defective'. Especially since the defect must be proven by the victim. If the basis for its assessment is the safety which a consumer is entitled to expect, what is the level of security that IoT users can expect from devices that are intrinsically vulnerable to cyber-attacks? (*ibid.*).

When discussing criminal cyber-activity, what comes first to mind are attacks on financial or tech companies and governments. However, a much simpler scenario, and sometimes overlooked, is to be considered: the health care industry. Medical technology has expanded to incorporate the Internet of Things, in what is now known as the 'Internet of Medical Things' (IoMT). This term refers to "*the ability of health care devices to communicate, gather, and exchange data across WiFi and Internet platforms*", ultimately providing "*up-to-date patient information, [enhancing] patient self-sufficiency, and [decreasing] the cost of care*" (Corbin, 2019, p. 1). The IoMT requires a legal framework that regulates the rights, responsibilities and obligations of the relevant stakeholders involved (*ibid.*). Even so, the European Union lacks comprehensive legal frameworks with a liability structure for hacks and breaches of IoMT devices that cause harm to its users.

All things considered, experts are witnessing the potential of IoT devices. Yet from a regulatory perspective the existing tools fail to give concrete answers to today's questions. The effectiveness of these legal frameworks cannot be entirely contested given the fact that they are still applicable and relevant. Nevertheless, their adequateness is put into question. Too many issues remain unclear, bringing about legal uncertainty to users and the industry. In particular, cyber-attacks and malicious cyber-activity, which are seldom – if at all – mentioned in liability regimes.

2.4. Policy considerations

The above sections have analyzed the EU liability acquis in relation to the Internet of Things, highlighting an imperative need for a more adequate regime vis-à-vis emerging digital technologies. In addition, it can be extrapolated that if the European Union truly wants to maximize the growth potential of the digital economy, proceeding to create a Digital Single Market, further harmonization in regulation is needed. At its core, harmonization translates into putting in agreement different ways of thinking which have developed over time in very diverse legal families. It is an arduous task but considering the possibility of creating a coherent overall system able to stimulate national legislation, could in the future, pave the way to a common European tort law. With this in mind, two options are available: (1) creating a new liability legal framework for emerging digital technologies; or (2) modifying the current liability framework – in particular the Product Liability Directive – so that it acknowledges the key features of new technologies with their respective risks.

Developing a new liability framework wouldn't imply repealing the PLD. On the contrary, it could be considered a *lex specialis*[27] in relation to it, enabling their interaction but offering more specific responses to technological advances. In that which regards the second option, a complete revision of the EU liability framework seems unjustified, although some adjustments need to be made to avoid situations in which victims – after suffering harm or damage caused by emerging technologies such as the IoT – remain totally or partially uncompensated. Generally speaking, irrespective of the alternative selected, specific areas need to be addressed in order to enhance legal certainty.

[27] *Lex specialis* (lex specialis derogat legi generali) is a principle of legal interpretation, as well as a method for solving conflicts between laws. It implies that specific rules have priority over general rules.

2.4.1. Updating definitions

Experts agree on the fact that definitions contained in the Product Liability Directive need to be updated or, at the very least, further clarified vis-à-vis new technological developments. To begin with, the notion of **'product'**. The interaction between tangible products and digital services is growing at a fast pace, blurring the separation line, a relevant example of that being software. Liability legal frameworks need to clarify under which category it falls – product, service or a brand new and independent category. For example, according to Regulation (EU) 2017/745 on Medical devices (2017, Preamble [19]):

> "[…] software in its own right, when specifically intended by the manufacturer to be used for one or more of the medical purposes set out in the definition of a medical device, qualifies as a medical device, while software for general purposes, even when used in a healthcare setting, or software intended for life-style and well-being purposes is not a medical device".

Further on there is the concept of **'producer'**. In this context, regulation must elucidate who the producer is in case of an update, upgrade or modification. Finally, the term **'damage'** should be more clearly delimitated to address the doubts on whether damage to data or digital assets is included. Considering the fact that data is one of the fundamental pillars of the digital reality, it should be incorporated in the notion of damage.

2.4.2. The defect

On the other hand, the meaning of **defect**, which tends to waver in relation to the IoT technology. It is assessed on the basis of the safety that a consumer is entitled to expect. This notion relates directly with the existence of safety standards for the IoT. However, in such ecosystems – mix of physical objects, software and services – establishing standards is challenging. The current gap is the lack of a holistic and more flexible approach. That is standards[28] do exist, but given the peculiarities of the technology, they

[28] Standards that ensure: a device can authenticate its user, encrypt data transfers, decrypt received data, deliver/verify the proof of existence, etc.

are not able to ensure its security (ENISA, 2018). Further work is needed to achieve "*an overarching approach that protects the entire IoT ecosystem*" (ibid., p. 4).

As IoT devices become more prevalent among consumers – in particular in the medical sphere – the safety expectations will increase. Although safety is a relative concept, because no product can be completely safe, further clarity is needed. The **development of new standards** could pave the way to safer devices and enlighten the notion of defect. In this way, courts could assess defective devices against pre-established standards.

In addition to the above, it would be useful to specify **when** the safety standard should be expected. In other words, if courts must assess expected safety when the device was placed on the market, and/or also when the device was updated.

2.4.3. The burden of proof

In many scenarios, legislators consider reversing the burden of proof with the underlying rationale of it being too burdensome for the victim. When discussing the IoT, a complex and opaque technology, most stakeholders[29] agree that proving the origin of the damage, the chain of events and overall who is to be held liable, is burdensome and expensive for the plaintiff. Consequently, obtaining compensation for damages is difficult and weakens the victim's position vis-à-vis the defendant. However, reversing the burden of proof would be disadvantageous for businesses. Producers could be held liable every time it's believed that the technology could not be controlled by the user. This could eventually lead to more litigation. Therefore, balancing all interests is essential in order to have a fair framework and avoid stifling innovation.

Under these circumstances, a more cautious approach would be advisable. Instead of completely reversing the burden of proof, a series of conditions that make eco of the challenges posed by the IoT technology could be introduced to alleviate the burden of proof. For example, the asymmetry of information or the likelihood of technological harm.

[29] Especially users, public authorities and civil society representatives.

2.4.4. Allocating liability in case of multiple parties

In light of the multiplicity of actors that coexist in IoT ecosystems, rules on how to allocate liability are in order. A strict liability framework appears as a reasonable regime for the IoT. Especially given the risks associated with new technologies, where often damage cannot be avoided. In this line, a good policy option seems to be that of holding all manufacturers jointly liable.

2.4.5. Limitations to liability

The «development risk defense» is included in many legal frameworks as an exception to liability. Yet, given the rate at which technological innovations appear on the market, it would be interesting to discuss if changes should be made to this clause or in relation to it. In particular, the possibility of including a post-market surveillance clause[30] for the manufacturer, that ensures some sort of safety monitoring obligation.

In like manner, it should be explored to which extent «**user fault**» could be relevant to limit or possibly exclude the producer's liability. For example, the incorrect use of the technology, lack of basic computer hygiene or failure to update the product's software when necessary.

2.4.6. Cyber-attacks

Finally, the subject of cyber-attacks and/or cyber-breaches, a growing issue that is affecting people worldwide. The importance of regulating this scenario at EU level is quite evident: cyber-attacks escape national boundaries. Accepting that the IoT, as well as other emerging technologies, are vulnerable does not necessarily imply that nothing can be done. Creating obligations in this area for manufacturers in terms of risk management, duty of care or the previously mentioned post-market surveillance and vigilance could improve European cybersecurity. In the same line, strengthening liability regimes so that damage suffered doesn't remain uncompensated has the potential to enhance consumer trust and to trigger cyber-security upgrades from the production stage.

[30] Already present in Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices which will enter into force on 26 May 2021.

Chapter 3: Insurance

Regulatory changes have an impact on society, therefore adopting a proactive stance in order to mitigate the risks of liability litigation is very much relevant. For some time now, special types of insurance policies have started to emerge – those which insure against cybercriminal activities – the so-called «**cybersecurity insurance**» or «**cyber risk insurance**». As the IoT technology advances and becomes more integrated in people's lives, its vulnerability generates risks. Although companies invest in activities that prevent or mitigate cybersecurity breaches – putting up firewalls, installing intrusion prevention and detection systems, encrypting data, developing training courses for employees, etc. – even the best cybersecurity cannot prevent all cyber-attacks. These are becoming increasingly sophisticated and difficult to detect. Therefore, businesses must invest in new risk mitigation strategies. This is part of a **holistic approach** towards safety and security which encompasses adopting preventive security mechanisms, but also a sort of 'incident response plan' that weighs in the financial consequences of a cyber-attack or data breach (Bodin *et al.*, 2018).

Cybersecurity insurance enables risk-sharing between customers and insurance companies. Chapter three will explore the role cybersecurity insurance can play in the creation of better incentives for safer behavior and in the convergence between security and safety in the digital sphere.

3.1. Introductory concepts

In essence, the insurance industry works by **transferring risks** of financial losses, big or small, through a contract (policy) from the insured – individual or entity with less ability to pay – to the insurer (insurance company). Such loss may emerge as a consequence of a damage to the insured or his/her property, or from liability for damage or injury caused to a third party (Kagan, 2020). Irrespective of its origin, insurance companies reimburse against the loss in exchange of a premium. People normally purchase insurance policies to protect themselves against accidents or other adverse events and, in certain situations, it is mandatory.

Insurance policies have three crucial elements: the premium, the policy limit and the deductible. The **premium** is the price of the policy, which is determined by the insurer

based on the industry or on the insured's risk profile (Kesan and Hayes, 2017). The **policy limit** is the maximum amount the insurer will reimburse per policy for a loss under its range of application. Such maximum amount may be established per period, loss or injury, or over the life of the policy – also known as lifetime maximum (Kagan, 2020). Higher coverage comes with a higher premium. Whereas the **deductible** is "*a specific amount the policy-holder must pay out-of-pocket before the insurer pays a claim*" (*ibid.*). They act as deterrents to "*large volumes of small and insignificant claims*" (*ibid.*).

Currently, commercial general liability policies are excluding cyber risk (Lyons and Nagashima, 2016). In light of this, insurance companies have started making available cyber risk insurance policies, specifically designed to "*respond to a number of losses due to a cyber-attack or data security breach*" (*ibid.*, p. 7).

3.2. Cybersecurity insurance: nature, market, coverage and challenges

Cybersecurity insurance is "*an insurance product designed to help businesses hedge against the potentially devastating effects of cybercrimes such as malware, ransomware, distributed denial-of-service (DDoS) attacks, or any other method used to compromise a network and sensitive data*" (CISCO, no date). It was born out of a raising awareness of cyber risks which, if left unaddressed, can potentially constrain the momentum created by digitization, affecting growth and prosperity worldwide (Hofmann, 2016).

According to experts, cyber risk has a **unique nature** in terms of severity, frequency and accumulation risk. Cyber-attacks can occur in any given moment, to one or multiple organizations simultaneously and/or repeatedly (Hofmann, 2016). Its reoccurrence being highly dependent on how fast the attack or breach was identified, analyzed and measures implemented, as well as on whether attackers will exploit new vulnerabilities. In fact, hackers are always looking for new weak points, because when a vulnerability is discovered and made public, it may become obsolete quickly (Siegel *et al.*, 2018). As for **accumulation risk**, it represents the vulnerabilities associated with companies using common platform software and relying on third-party solutions – for example using the cloud (*ibid.*). All in all, it is the "*total exposure affected by incidents […] that could cause a significant business disruption or loss across geographies or companies, and affect several insurance policies*" (Siegel *et al.*, 2018, p. 12). Its relevance is often overlooked

by the general public, but with interconnectivity and cloud service usage increasing, its potential impact becomes more and more worrisome.

In this challenging context the insurance industry saw an opportunity to create new solutions, helping customers to improve their risk mitigation strategies. This **market** remains relatively **immature** for a series of reasons: 1) lack of standardization of insurance offerings; 2) first-time cyber insurers offering limited policies; 3) new entrants to the market providing services that may not be sufficiently robust or adequate (Siegel *et al.*, 2018). The lack of standardization of insurance offerings leads to different practices. With some insurers clearly separating traditional policies from cyber insurance ones, whereas others embed it in existing coverage[31]. The choice of including it in a normal policy may pose issues in terms of clearly understanding what is covered or not. Defining and delimitating coverage, in fact, is difficult giving the evolving nature of cyber risk (Siegel *et al.*, 2018). In that which regards first-time cyber insurers two considerations emerge. Firstly, they focus on common cyber risk events, offering limited policies, because of lack of experience in the area (e.g. access to data, pricing mechanisms, risk modelling tools, etc.). They need to improve their expertise in order to expand their offer. Secondly, these limited services may not be as robust or adequate vis-à-vis a cyber incident as those of their more experienced competitors (*ibid.*).

Notwithstanding, it is the **fastest growing line of business** in the industry (Hofmann, 2016). The U.S. market positioned as leader – with premiums ranging from 1.5 to 2 billion dollars annually – while Europe and Asia "*are catching up due to new regulations and recent attacks*" (Siegel *et al.*, 2018, p. 24). In fact, European insurers are developing offers that target European priorities, regulations and cultural norms, in particular, the GDPR (*ibid.*). Current forecasts indicate that premiums may reach **20 billion dollars in 2025** (Bernardino, 2019). The reason behind the cyber insurance market's profitability is the limited number of existing claims. Nevertheless, such profitability is expected to stabilize when the balance between regulation and claims incurred changes in the future (Siegel *et al.*, 2018).

Notwithstanding the above, the delimitation of the cybersecurity insurance policy's coverage "*will necessarily be subject to the insurer's overall risk appetite and ability to*

[31] i.e. Stand-alone cyber insurance and 'package' or endorsed cyber coverage.

quantify the nature and extent of the risks it is assuming" (*ibid.*, p. 7). Some policies may cover first-party losses – i.e. the company's own damages that originated from cyber losses – and/or third-party losses – i.e. liability protection in case of damage to a third-party. According to McMillan (Lyons and Nagashima, 2016), a cyber liability insurance policy that has been tailored to the client's needs may cover: income loss after an incident (whether it's a cyber-attack or privacy/data security breach); loss of the profits that would've been earned if the incident hadn't happened; business interruption associated expenses; notification costs for privacy and data security breaches, as well as related legal costs and, if applicable, costs related to monitoring the credit of affected customers and/or others for a period of time following the incident; costs incurred to avoid claims that, if made, would be covered under the policy; if legally allowed, costs of regulatory actions and investigations; fines and/or penalties; third-party legal liability from hacking, malware or breaches to privacy or data security; and cyber extortion[32]. Whereas an OECD report highlights that the most common type of coverage is "*compensation for incident response costs and privacy breaches, data and software losses and business interruption*" (Bernardino, 2019, p. 3). However, according to Bernardino (*Ibid.*), some of the most relevant corporate needs, such as "*coverage for reputational damage or intellectual property theft, are rarely included in cyber risk insurance*".

The Geneva Association (see Siegel *et al.*, 2018), leading international think tank of the insurance industry, highlights that cyber insurance companies are offering in their policies much more than compensation for potentially significant financial losses – known as risk transfer possibilities. Their business model is transforming to include additional services[33] along the value chain: pre-breach and post-breach. The '**pre-breach services'** include risk consultation and prevention packages. That is, they work with clients so that they understand risks and use adequate risk management frameworks to prevent breaches. But also, offer services to train companies' staff in cyber-attack/cyber incident response scenarios – i.e. how to react and limit damages, and what are the best practices. Whereas the '**post-breach services**' are meant to help the client evaluate the impact of an attack (enabling access to specialized experts[34]), implement an appropriate response plan and

[32] Generally known as ransomware.
[33] These new services are provided normally through partnerships.
[34] It may include access to IT forensic experts, as well as legal or crisis communications support. This is the case of Allianz.

recover. This is in line with a **holistic approach to cybersecurity**, which represents a change in paradigm. In fact, traditionally, insurance companies were present only after a breach (*ibid.*). In this new context, insurance companies help their customers build and/or improve cyber resilience, while effectively preparing staff to mitigate the negative impacts generated by an incident. The new role adopted by this industry is motivated by three concrete market needs: 1) the growing attractiveness of cybersecurity insurance for customers; 2) improving profitability by reducing and/or preventing losses and increasing client retention/loyalty; 3) gaining cyber risk knowledge, which translates into a competitive advantage for insurers (Siegel *et al.*, 2018, p. 19).

These present-day offerings, however, are not free of challenges. In part because of cyber risk's unique nature and accumulation risk, and in part because – to this date – it still is **not well understood** by either insurers or their customers. The need for a deeper understanding of cyber risk is a core challenges for clients[35] – because they don't comprehend the available products nor their own needs – and for underwriters and/or brokers – because they lack specialized expertise, and thus, don't comprehend fully the risks involved (EIOPA, 2018).

There is **inadequate actuarial data**, as well as **asymmetry of information** between insurers and those seeking insurance (Bodin *et al.*, 2018). This prompts problems when designing cyber risks models which help improve pricing methodology and identify shortcomings in security. The lack or insufficiency of historical data, on the frequency and severity of cyber incidents, represents an obstacle in the **quantification** of certain **cyber risks**. Consequently, insurance companies act prudently when designing policies, establishing exclusions and/or limits, in order to control or mitigate their range of exposure (Bernardino, 2019). Furthermore, some insurers "*are overly conservative in pricing their cybersecurity premiums because they fear the occurrence of a "cyber hurricane", in which the insurance company is overwhelmed by claims due to correlated risks*" (Bodin *et al.*, 2018, p. 528).

In addition, there is an issue with **awareness** of cybersecurity related vulnerabilities. Since there is not a common database of incident data, companies don't fully comprehend their level of exposure. The difficulty with data sharing lies on the fact that businesses

[35] Observed especially in SMEs.

don’t want to be subject to more attacks, regulatory fines, legal fees or reputational damage (Siegel *et al.*, 2018). It is important to note, in this case, the role l**egal frameworks** play in improving the availability of data. As a matter of fact, the European Union’s GDPR, by strengthening the protection on personal data, has triggered demand for cyber risk coverage in insurance policies (Bernardino, 2019). But also, by rendering mandatory the notification of cyber incidents is enabling the improvement of actuarial data. Experts estimate that in the future there may be parity between the American and the European cyber insurance market, mainly because of the implementation of the GDPR (*ibid.*). Notwithstanding, harmonizing cyber incidents’ related information requires public and private collaboration.

3.3. Safety and Security

In order to determine the role cybersecurity insurance can play in the creation of better incentives for safer behavior and in the convergence between security and safety in the digital sphere, further clarification is needed. Safety and security are two terms often used interchangeably – in some languages only one word exists to mean both – but they are quite distinct.

Digital safety is “*the protection of the user in his or her environment, with technical mechanisms and policies that protect the users from being harmed by improper operation of the device*” (Cerf *et al.*, 2016, p. 10). Whereas **online security** is “*the protection of the physical network, operating systems and content from exposure, modification or functional damage, utilizing a combination of software and hardware mechanisms*” (*ibid.*). While in digital safety the focus is on the end user and its interests, in online security the focus is on protecting other parts of the network or the device.

Reasoning about safety – one of the EU public policy objectives – most definitely implies considering **risk**. In fact, the notion of product safety within the European Union “*encompasses protection against all kinds of risks arising from the product, including not only mechanical, chemical, electrical risks but also cyber risks and risks related to the loss of connectivity of devices*” (European Commission, 2020a, p. 6). This concept is also linked to the use of the product, that is, the intended use, but also the foreseeable use and, in certain cases, the reasonably foreseeable misuse (*ibid.*). The overall aim is to offer better protection to all users.

Some authors describe safety as "*the absence of unreasonable risk*" – its reasonableness being defined by the series of measures taken to prevent a mishap (Miller, 2017, p. 85). In order to determine safety, the risk of harm to people must be determined (*ibid.*). While evaluating risk exposure, **safety requirements** must also be established for each life cycle phase – i.e. design, manufacturing, maintenance and disposal – in order to reduce such risk (*ibid.*, p. 87). The difficulty lies in striking a balance between measuring risk while remaining sensitive to changes in the perception of risk (*ibid*., 95).

The concept of 'safety' is not new, yet it becomes "*exponentially more widespread as connectivity continues to involve more physical spaces*" (*ibid.*, p. 12). Given the fact that the Internet is a shared environment, and that there is a growing number of IoT devices connected to the internet, its governance becomes a **shared responsibility**. The private sector must secure user trust, upgrading security measures so that users remain safe from online dangers. As well, it must educate users on how best to use available tools. Governments must put in place regulation to deter and punish inappropriate online behavior and enforce norms (Cerf *et al.*, 2016), but also educate citizens in basic computer hygiene. Civil society must continue analyzing and evaluating private-sector practices so that laws and principles for online behavior can be established. Its role is essential in making sure that checks and balances for governmental institutions are working properly and keeping up with technological innovation (*ibid.*). The technical community must ensure that standards are being updated and that new protections and best practices are implemented. Similarly, it must contribute to the education of the general public. But most importantly, users must be responsible and learn to use the tools which enable a safer and more secure experience in the digital sphere (*ibid.*).

The IoT ecosystems are complex, connecting virtually any machine or object, and configured to send data collected to cloud applications. Among the special cybersecurity challenges posed by the IoT is that it was not designed for security, but rather for convenience (Vitkowsky, 2015). Therefore, digital security risks are abundant, with hackers taking advantage of any given vulnerability (Thales, 2019). Privacy and data security are some of the main issues, addressed in Europe by the GDPR. Yet, challenges also emerge in light of possible bodily injury and/or property damage. This is linked to any device malfunction that causes real damage in the physical world – a new window for cyber liabilities (Vitkowsky, 2015). Because of the characteristics of the technology

– the diversity of devices and data types used – **no «one size fits all» solution can be applied**.

It is quite clear that, in the face of cyber risk, any IoT business must necessarily go through a thorough security risk assessment in order to put in place cybersecurity strategies for the entire lifecycle of the product. As a matter of fact, four common options are available to address cyber risks: 1) avoid the risk; 2) retain the risk; 3) self-protect and mitigate the risk; and 4) transfer the risk (Bolot and Lelarge, 2008). The first option is unrealistic in this era of the Fourth Industrial Revolution and advanced technological innovation – risk cannot be avoided. The second option – accepting loss when it materializes – is feasible only in certain scenarios since the entity of the damage varies from breach to breach. Option three involves investing in ways to reduce or mitigate "*the impact of the risk and the severity of the damages*" (*ibid.*, p. 2). Whereas the last option deals with risk transferring mechanisms. Traditionally the focus has been on options 2 and 3. However, as Bolot and Lelarge (2008, p. 2) point out, "*self protecting against risk or mitigating risk does not eliminate risk*"[36]. Whatever the resources invested in cybersecurity, there is always a **residual risk**. At the present time, only cyber insurance policies handle the risk transfer considered in option four. All things considered, experts believe insurance to be *a "**powerful mechanism** to promote network-wide changes and lead all users of the network to the desirable state where they all invest in self-protection*" (Bolot and Lelarge, 2008, p. 16). Even though quantifying risks – to establish the premium – is an arduous task[37], the insurance industry has been dealing with similar issues in other areas for decades or centuries. Indeed, even insurance for pandemics exists nowadays.

For the most part, cyber insurance appears to be a good policy option to incentivize safer behavior. Three independent pillars exist for a safety process – 1) policy, 2) audit and assessment, and 3) implementation (Miller, 2017, p. 91). Insurance intervenes in auditing and assessing risk within enterprises and implementing mitigation strategies pre and post breach. These are valuable incentives to modify unsafe practices. The implementation of a **holistic risk management approach** by insurance companies is, in fact, beginning to

[36] As Bolot and Lelarge explain, there are limits to the detection and identification mechanisms for threats. In fact, cybercriminals and the threats they produce, evolve on their own and in response to the deployment of detection and mitigation solutions, thus hindering those strategies.
[37] For a series of reasons, i.e. the protected assets are intangible, damages emerge only after threats/attacks were identified, risks vary at great speed, etc.

pave the way towards convergence between safety and security in the digital sphere. In fact, according to the World Economic Forum (2018, p. 58), an increment in the adoption of cyber insurance policies is likely to "*result in short term costs but* ***long term reduction of cyber incident related damages***". In the same line, it is likely to "***improve security*** *as insurers insist on security controls to minimize downside risk arising from cyber-related claims or begin bundling security with insurance provision*" (*ibid.*). Accountability is also expected to increase, as the process through which businesses go to obtain insurance elucidates "*the risks and who bears the cost of risk management*" (*ibid.*).

To conclude, these risk management plans, equipped with risk prevention and resolution tools, access to experts (cyber, communications, legal, etc.) and learning opportunities for staff, better prepare clients to deal with cyber risk. A holistic approach to online safety and security allows the emphasis to fall, not on the quality of a specific measure on a single part of the chain, but rather on the role that all stakeholders have in the digital sphere. Otherwise there is failure to see all the vulnerabilities, and risks of hacking or breaches increase significantly. Overall, insurance is becoming an essential component of risk management in the digital world.

Conclusions

At the core of this dissertation was cybersecurity in terms of EU liability regulation and the use of insurance. One of the research questions was whether the EU liability legal framework was adequate and efficient vis-à-vis new technological developments. If the answer was negative (in both scenarios or only one), how could liability be allocated adequately and/or efficiently in this legal context? Whereas, the final part of this thesis explored cyber insurance to determine if it could incentivize safer behavior and if it could be used to work towards convergence between security and safety in the digital sphere.

Upon careful consideration, the following conclusions can be presented:

I. The Paradox of Progress

Society faces the paradox of progress. Digitization, digitalization and the digital transformation have paved the way to a more efficient and connected world. They've also generated new opportunities for a better future and improved wellbeing. Yet, increased connectivity has translated into building a fragile system, with inherent vulnerability problems growing in our infrastructures, economies and politics.

II. A Common Societal Challenge

Cybersecurity related issues require increased awareness of the fact that society faces a common challenge that can only be solved in a collective manner. For this reason, all stakeholders must be involved and rise to the challenge responsibly.

Although accomplishing public-private collaboration has its difficulties, it is necessary to open the discussion and frame it on five key values: security, privacy, economic value, accountability and fairness. In the same line, beginning to discuss regulation on emerging technologies at an international level can help States in the elaboration of standards and rules on thorny subject areas which they will be forced to regulate at a national level eventually.

Moreover, it is necessary to invest in digital literacy training, so that basic computer hygiene becomes a daily habit, and security measures aren't rendered futile by individuals' carelessness – considered to be the weakest link in the security chain.

III. Existing Liability Regulatory Framework

At present, there is no specific EU nor specific national regulatory framework regarding liability in the context of the Internet of Things. If EU citizens and/or businesses were currently confronted with liability issues caused by IoT devices, they would fall back upon the existing general regulatory framework.

At EU level, stakeholders are mainly dependent on the Product Liability Directive – one of the most important examples of EU liability harmonization. Apart from a few exceptions, the rest is mostly non-harmonized and dependent on national legislation. In fact, from the analysis emerges a reliance, in this field, on the parallel application between EU law and national law.

At national level, Member States do not have in place liability rules specifically applicable to damage resulting from the use of emerging digital technologies. The only exceptions are for automated vehicles. Generally, Member States continue to use their own liability regimes, in combination with EU regulation, and resort to legal analogy when necessary. Although these frameworks may still be efficient and relevant, the existing gaps for an emerging technology such as the IoT is uncontestable. Overall, litigation for victims – in cases where IoT devices are involved – appear to be burdensome, time-consuming and expensive.

IV. Effectiveness of the Liability Regulatory Framework

European surveys and further analysis could not conclude on the effectiveness or ineffectiveness of the Directive vis-à-vis technological developments. The lack of concrete evidence of real-life problems or cases makes it a contested subject.

V. Adequateness of the Liability Regulatory Framework

The current legal base is not sufficiently adequate – given the features and characteristics of IoT devices – to address problems posed by this emerging technology. In fact, a majority of stakeholders agrees that the issue of technological developments is not adequately covered by the Product Liability Directive. In brief, the scope and definitions of the PLD create certain legal uncertainty in the context of the IoT, in particular, in the case of software. But also, the added complexity of the technology, which incorporates more components and, consequently more actors,

render identifying the origin of the damage and allocating liability, to say the least, challenging.

Furthermore, at national level, the absence of definitions or regulation for new concepts, actors or relations could catalyze the analogical application of vicarious liability for operators of machines, computers, robots, etc., in those legal frameworks that support it. This could prompt major legal uncertainty issues for operators, possibly hindering (to a certain extent) innovation.

Another shortcoming of the liability regulatory framework is the absence of mentions to cyber-attacks and malicious cyber-activity. Consequently, assessing reasonable and appropriate levels of cybersecurity and due care presents multiple difficulties.

VI. EU Liability Regulatory Framework – considerations

Two policy options are available, if doing nothing can be excluded: (1) creating a new liability legal framework for emerging digital technologies; or (2) modifying the current liability framework – in particular the Product Liability Directive – so that it acknowledges the key features of new technologies with their respective risks.

A new liability framework would act as *lex specialis*, interacting with the PLD yet offering more precise answers to damages emergent from new technological advances. Whereas, the modification of the current liability framework would imply making targeted adjustments, with no need for a complete revision.

Notwithstanding the course of action chosen, specific areas need to be addressed in order to enhance legal certainty. In particular: updating definitions; better delimiting the notion of defect and associated safety considerations/standards; revising the conditions upon which the burden of proof can be alleviated vis-à-vis the new features of emerging technologies; determining rules for allocation of liability in cases of multiple actors, such as holding all manufacturers jointly liable; further discussing changes to the «development risk defense» clause, in terms of possibly adding a post-market surveillance clause; exploring the relevance of «user fault»; and including cyber-attack scenario related regulation – creating obligations for manufacturers of risk management, duty of care or even post-market surveillance and vigilance.

VII. Insurance

There is no specific regulation regarding cyber insurance in the context of the IoT. Although it remains an immature market, it is the fastest growing line of business in the industry. The unique nature of cyber risk, the accumulation risk, the low awareness of cybersecurity related vulnerabilities, the lack of actuarial data, as well as the asymmetry of information between customers and insurers pose multiple challenges to its development. All in all, cyber insurance represents a change in paradigm for the insurance industry. It signals the endorsement of a holistic approach to cybersecurity in which additional services are offered to clients: pre-breach and post-breach.

Cyber insurance materializes as a good policy option to incentivize safer behavior. Cyber resilient clients are rewarded with lower premiums, and the implementation of a holistic risk management approach paves the way towards convergence between safety and security in the digital sphere. Further analysis should be carried out in terms of discussing the possibility of rendering cyber insurance compulsory in certain scenarios.

To conclude, European Union citizens are entitled to the same level of protection and rights, irrespective of whether they suffer harm from an IoT device or not, and/or if it materializes in the physical or digital sphere. Current liability regulatory frameworks present gaps that must be addressed in favor of greater legal certainty. Finally, cybersecurity is a challenge that can only be undertaken collectively with a holistic approach. All available methods must be used to increase awareness of the issues faced, incentivize safer online behavior, and produce more secure devices and systems. Cyber insurance appears to be one of these methods, but other options should be discussed and implemented.

Bibliography

Agrawal, T. *et al.* (2014). "JPMorgan hack exposed data of 83 million, among biggest breaches in history," *Reuters*, 3 October. Available at: https://www.reuters.com/article/us-jpmorgan-cybersecurity/jpmorgan-hack-exposed-data-of-83-million-among-biggest-breaches-in-history-idUSKCN0HR23T20141003 (Accessed: April 21, 2020).

Bernardino, G. (2019). *Keynote speech: Cyber Security and Cyber Risk: A universal Challenge*, [online] 26 February. Available at: https://bit.ly/2BTCOAw (Accessed: June 25, 2020).

Bodin, L. D. *et al.* (2018). Cybersecurity insurance and risk-sharing. *Journal of Accounting and Public Policy*, [e-journal] 37(6), pp. 527–544. Available at: https://doi.org/10.1016/j.jaccpubpol.2018.10.004 (Accessed: June 21, 2020).

Bolot, J. and Lelarge, M. (2008). *Cyber Insurance as an Incentive for Internet Security*. Hanover NH. Available at: https://www.di.ens.fr/~lelarge/papiers/2008/cyber-surv.pdf (Accessed: July 3, 2020).

Brous, P., Janssen, M. and Herder, P. (2020). The dual effects of the Internet of Things (IoT): A systematic review of the benefits and risks of IoT adoption by organizations. *International Journal of Information Management*, [e-journal] 51(May). Available at: https://doi.org/10.1016/j.ijinfomgt.2019.05.008 (Accessed: May 18, 2020).

Cerf, V. G. *et al.* (2016). IoT safety and security as shared responsability. *Business Informatics*, [e-journal] 1(35), pp. 7–19. doi: 10.17323/1998-0663.2016.1.7.19. (Accessed: July 3, 2020).

CISCO (no date). *What Is Cyber Insurance?*, *Cyber Security and Insurance*. Available at: https://bit.ly/3gDhZI8 (Accessed: June 24, 2020).

Corbin, B. A. (2019). When 'things' go wrong: Redefining liability for the Internet of Medical Things. *South Carolina Law Review*, [e-journal] 71(1). Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3375070. (Accessed: June 14, 2020).

Deloitte (2020). *Tech Trends 2020*, *Deloitte Insights*. s.l.: Deloitte. Available at: https://www2.deloitte.com/us/en/insights/focus/tech-trends.html. (Accessed: May 18, 2020).

Donalds, C. and Osei-Bryson, K. M. (2020). Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. *International Journal of Information Management*, [e-journal] 51(December), pp. 1–16. Available at: https://doi.org/10.1016/j.ijinfomgt.2019.102056. (Accessed: May 19, 2020).

EIOPA (2018). *Understanding Cyber Insurance-A Structured Dialogue with Insurance Companies*. Luxembourg: Publications Office of the European Union. doi: 10.2854/223306. (Accessed: June 25, 2020).

Elischer, D. (2017). Wrongfulness As a Prerequisite Giving Rise to Civil Liability in European Tort Systems. *Common Law Review, Forthcoming*, [e-journal] (March 17), pp.

1–16. Available at: http://dx.doi.org/10.2139/ssrn.2934912 (Accessed: May 26, 2020).

Engelke, P. (2018). Three ways the Fourth Industrial Revolution is shaping geopolitics. *World Economic Forum*, [online] Available at: https://bit.ly/2BNqGBc (Accessed: May 23, 2020).

ENISA (2018). *IoT Security Standards Gap Analysis. Mapping of existing standards against requirements on security and privacy in the area of IoT*. s.l.: ENISA. doi: 10.2824/713380. (Accessed: June 16, 2020).

European Commission (2016). *Advancing the Internet of Things in Europe* (SWD(2016) 110 final). Available at: https://bit.ly/2VZ2LWf (Accessed: June 15, 2020).

European Commission (2017). *Digital Single Market. EU cybersecurity initiatives working towards a more secure online environment*. Available at: https://bit.ly/3fbjYTT (Accessed: April 19, 2020).

European Commission (2018a). *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*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018SC0157 (Accessed: May 27, 2020).

European Commission (2018b). *Liability for emerging digital technologies*. SWD(2018) 137 final. Available at: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52018SC0137 (Accessed: April 14, 2020).

European Commission (2019). *Supporting telecommunications networks and digital service infrastructures across Europe*. EUR-Lex, [online] Available at: https://eur-lex.europa.eu/legal-content/en/LSU/?uri=CELEX%3A32014R0283 (Accessed: May 28, 2020).

European Commission (2020a). *Report on the safety and liabaility implications of Artificial Intelligence, the Internet of Things and robotics*. Available at: https://ec.europa.eu/info/sites/info/files/report-safety-liability-artificial-intelligence-feb2020_en_1.pdf (Accessed: April 14, 2020).

European Commission (2020b). *Shaping Europe's digital future* COM(2020) 67 final. Available at: https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf (Accessed: April 14, 2020).

Expert Group on Liability and New Technologies (2019). *Liability for Artificial Intelligence and other emerging digital technologies*. doi: 10.2838/573689. (Accessed: April 14, 2020).

Gartner (2017). *Leading the IoT - Gartner Insights on How to Lead in a Connected World*, *Gartner*. doi: 10.1038/sj.emboj.7600210. (Accessed: May 21, 2020).

Goodman, M. (2015). *Los delitos del futuro*. 2nd ed. New York: Ariel.

Hofmann, D. M. (2016). *Cyber Insurance as a Risk Mitigation Strategy. Contours of an emerging market for cyber risk transfer*. Geneva: Geneva Association. Available at: https://bit.ly/2Zg6hxj (Accessed: June 24, 2020).

Interpol (2020). *COVID-19 cyberthreats*. Available at: https://www.interpol.int/Crimes/Cybercrime/COVID-19-cyberthreats (Accessed: April 20, 2020).

ISO/IEC (2012). *ISO/IEC 27032:2012, Information technology — Security techniques — Guidelines for cybersecurity*. Available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en (Accessed: April 20, 2020).

Kagan, J. (2020). "Insurance Definition," *Investopedia*, [online]. Available at: https://www.investopedia.com/terms/i/insurance.asp (Accessed: June 23, 2020).

Kammel, B., Pogkas, D. and Benhamou, M. (2019). These Are The Worst Cyber Attacks Ever. *Bloomberg*, [online] March 18. Available at: https://bloom.bg/2BNMRat (Accessed: April 21, 2020).

Kesan, J. P. and Hayes, C. M. (2017). Strengthening Cybersecurity with Cyberinsurance Markets and Better Risk Assessment. *Minnesota Law Review*, [online] 85. Available at: https://scholarship.law.umn.edu/mlrhttps://scholarship.law.umn.edu/mlr/85 (Accessed: June 23, 2020).

Khan, W. Z. *et al.* (2016). Enabling Consumer Trust Upon Acceptance of IoT Technologies Through Security and Privacy Model, in Park, J. J. et al. (eds.) *Lecture Notes in Electrical Engineering. Advanced Multimedia and Ubiquitous Engineering*. Springer, [online] pp. 111–117. doi: 10.1007/978-981-10-1536-6. (Accessed: June 13, 2020).

Koziol, H. (2015). Comparative Conclusions. Part 6 The elements of liability, in Koziol, H. (ed.) *Basic Questions of Tort Law from a Comparative Perspective*. Vienna: Jan Sramek Verlag, p. 781. Available at: www.jan-sramek-verlag.at (Accessed: May 26, 2020).

Lipton, D. (2018). Trust and the Future of Multilateralism. *International Monetary Fund*, [online]. Available at: https://www.imf.org/en/News/Articles/2018/04/30/sp042618-trust-and-the-future-of-multilateralism (Accessed: May 23, 2020).

Lyons, C. and Nagashima, J. (2016). Mitigating Cyber Risk and Cybersecurity Insurance. *McMillan*, [online] (May), pp. 1–10. Available at: https://www.mcmillan.ca/Files/188597_Mitigating Cyber Risk and Cybersecurity Insurance.pdf. (Accessed: June 23, 2020).

Machnikowski, P. (2016). "Conclusions", in Machnikowski, P., ed., *European Product Liability: An Analysis of the State of the Art in the Era of New Technologies*. Intersentia, pp. 669–705. doi: https://doi.org/10.1017/9781780685243.

Miller, J. D. (2017). "The Business of Safety," in Griffor, E., ed., *Handbook of System Safety and Security*. Elsevier Inc., pp. 81–94. doi: 10.1016/B978-0-12-803773-7.00005-X.

Morgan, S. (2018). Global Cybercrime Damages Predicted To Reach $6 Trillion Annually By 2021. *Cybersecurity Ventures Cybercrime Magazine*, [online] December 7. Available at: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/ (Accessed: May 21, 2020).

Pagliery, J. (2015). JPMorgan's accused hackers had vast $100 million operation. *CNN Business*, [online] November 10. Available at: https://money.cnn.com/2015/11/10/technology/jpmorgan-hack-charges/ (Accessed: April 21, 2020).

Perlroth, N. (2017). All 3 Billion Yahoo Accounts Were Affected by 2013 Attack. *The New York Times*, [online] October 3. Available at: https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html (Accessed: April 21, 2020).

Pupillo, L. (2018). EU Cybersecurity and the Paradox of Progress. *CEPS Policy Insights*, [e-journal] February(2018–06), pp. 1–8. Available at: https://www.ceps.eu/download/publication/?id=10432&pdf=PI2018_06_LP_ParadoxProgress.pdf. (Accessed: April 14, 2020).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) (2016) *Official Journal* L 119, 4.5.2016, p. 1-88. Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj#d1e3383-1-1 (Accessed: June 11, 2020).

Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Text with EEA relevance) (2017) *Official Journal* L 117, 5.5.2017, p. 1-175. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R0745 (Accessed: June 17, 2020).

Repubblica, (2019). Unicredit, attacco informatico: violati i dati per 3 milioni di utenti nel 2015. 'Nessun accesso ai conti'. *La Repubblica*, [online] October 28. Available at: https://www.repubblica.it/economia/2019/10/28/news/unicredit_dati-239711077/ (Accessed: April 21, 2020).

Schwab, K. (2016). The Fourth Industrial Revolution: what it means and how to respond. *World Economic Forum*, [online] January 1. Available at: https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/ (Accessed: April 14, 2020).

Shull, A. (2019). "Governing Cyberspace during a Crisis in Trust," in *Governing Cyberspace during a Crisis in Trust. An essay series on the economic potential — and vulnerability — of transformative technologies and cyber security*. Waterloo: Centre for International Governance Innovation, pp. 4–8. Available at: https://www.cigionline.org/cyberspace (Accessed: May 19, 2020).

Siegel, M. *et al.* (2018). *Cyber Insurance as a Risk Mitigation Strategy*. The Geneva Association. Available at: https://www.genevaassociation.org/research-topics/cyber-and-innovation/cyber-insurance-risk-mitigation-strategy. (Accessed: June 24, 2020).

Studer, E. and De Werra, J. (2017). Regulating cybersecurity. What civil liability in case of cyber-attacks?. *Expert Focus 8/2017*, (August), pp. 511–517. Available at: https://ssrn.com/abstract=3022522. (Accessed: June 9, 2020).

Thales (2019). *Securing the IoT - Building trust in IoT devices and data*. [online] Available at: https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/iot-security (Accessed: July 3, 2020).

The Guardian (2018). Hackers steal data of 150 million MyFitnessPal app users. *The Guardian*, [online] March 30. Available at: https://www.theguardian.com/technology/2018/mar/30/hackers-steal-data-150m-myfitnesspal-app-users-under-armour (Accessed: April 21, 2020).

US National Intelligence Council (2017). *Global Trends. The Paradox of Progress*, *Bmj*. doi: 10.1136/bmj.310.6991.1418. (Accessed: April 20, 2020).

Vengattil, M. and Dave, P. (2018). Facebook now says data breach affected 29 million users, details impact. *Reuters*, [online] October 12. Available at: https://reut.rs/3edwAss (Accessed: April 21, 2020).

Vitkowsky, V. J. (2015). The Internet of Things : A New Era of Cyber Liability and Insurance. *International Association of Claim Professionals*, Declaratio(Spring), pp. 15–17. Available at: https://litigationconferences.com/wp-content/uploads/1955/12/Are-You-and-Your-Insurer-The-Internet-of-Things.pdf (Accessed: April 21, 2020).

Warf, B. (2018). "Cybersecurity," *The SAGE Encyclopedia of the Internet*. doi: http://dx.doi.org/10.4135/9781473960367.n50. (Accessed: July 3, 2020).

WEF (2019). *Global Risks Report 2019*. Geneva: World Economic Forum. Available at: http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf. (Accessed: April 19, 2020).

WEF (2020). *The Global Risks Report 2020*. Geneva: World Economic Forum. Available at: http://wef.ch/risks2019. (Accessed: May 21, 2020).

WEF (no date). *Shaping the Future of Cybersecurity and Digital Trust*, *World Economic Forum*. [online] Available at: https://www.weforum.org/platforms/shaping-the-future-of-cybersecurity-and-digital-trust (Accessed: May 18, 2020).

WEF and Boston Consulting Group (2018). *Cyber Resilience Playbook for Public-Private Collaboration*, *Cyber Resilience Playbook for Public- Private Collaboration*. Geneva: World Economic Forum. Available at: http://www3.weforum.org/docs/WEF_Cyber_Resilience_Playbook.pdf. (Accessed: May 22, 2020).

Wolford, B. (no date). *What is GDPR, the EU's new data protection law? GDPR.eu* [online]. Available at: https://gdpr.eu/what-is-gdpr/ (Accessed: June 10, 2020).

Wolters Kluwer (no date). "Daños y perjuicios," *Guias Juridicas Wolters Kluwer*. Available at: https://bit.ly/3iQ6xL9 (Accessed: May 25, 2020).

World Customs Organization (2019). *Study report on disruptive technologies*. Available at: https://bit.ly/2ZPwhyM (Accessed: May 18, 2020).