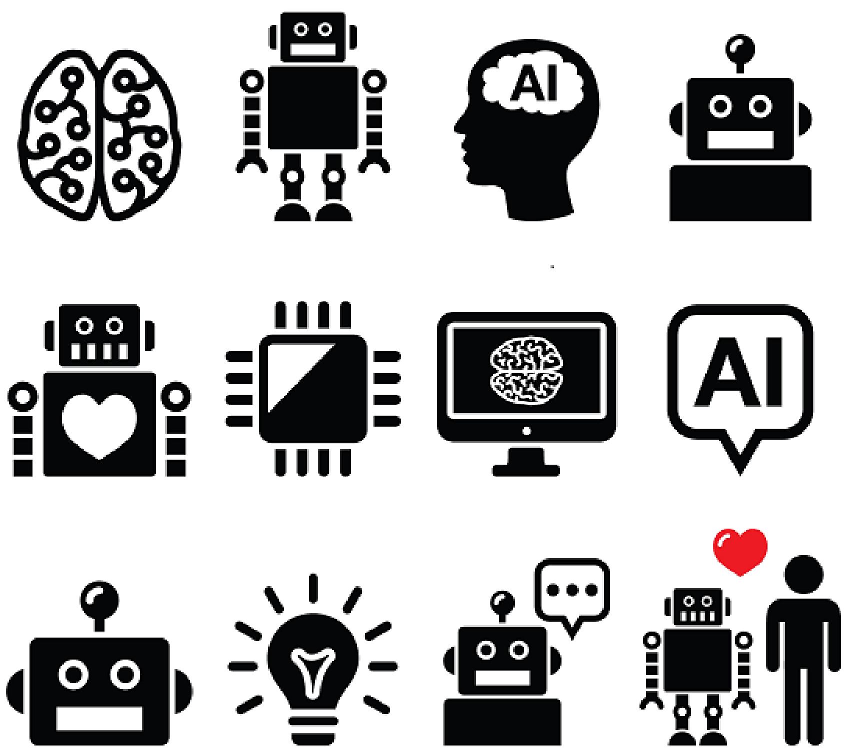
STUDY

Requested by the JURI committee

European Parliament

# Artificial Intelligence and Civil Liability

## Legal Affairs




Policy Department for Citizens' Rights and Constitutional Affairs
Directorate-General for Internal Policies
PE 621.926 - July 2020

EN

# Artificial Intelligence and Civil Liability

## Legal Affairs

**Abstract**

This study – commissioned by the Policy Department C at the request of the Committee on Legal Affairs – analyses the notion of AI-technologies and the applicable legal framework for civil liability. It demonstrates how technology regulation should be technology-specific, and presents a Risk Management Approach, where the party who is best capable of controlling and managing a technology-related risk is held strictly liable, as a single entry point for litigation. It then applies such approach to four case-studies, to elaborate recommendations.

This document was requested by the European Parliament's Committee on Legal Affairs.

**AUTHORS**
Andrea BERTOLINI, Ph.D., LL.M. (Yale)
Assistant Professor of Private Law, Scuola Superiore Sant'Anna (Pisa)
Director of the Jean Monnet - European Centre of Excellence
on the Regulation of Robotics and AI (EURA)
www.eura.santannapisa.it
andrea.bertolini@santannapisa.it

**ADMINISTRATOR RESPONSIBLE**
Giorgio MUSSA

**EDITORIAL ASSISTANT**
Sandrina MARCUZZO

**LINGUISTIC VERSIONS**
Original: EN

**ABOUT THE EDITOR**
Policy departments provide in-house and external expertise to support EP committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny over EU internal policies.

To contact the Policy Department or to subscribe for updates, please write to:
Policy Department for Citizens' Rights and Constitutional Affairs
European Parliament
B-1047 Brussels
Email: Poldep-Citizens@ep.europa.eu

Manuscript completed in July 2020


This document is available on the internet at:
http://www.europarl.europa.eu/supporting-analyses

# CONTENTS

# LIST OF ABBREVIATIONS

| | |
|---|---|
| **AI** | Artificial Intelligence |
| **AI HLEG** | High-Level Expert Group on Artificial Intelligence |
| **AD** | Automated Driving |
| **ADS** | Automated Driving Solutions |
| **Art.** | Article |
| **BGB** | German Civil Code |
| **CAD** | Connected and Automated Driving |
| **CbC** | Class-of-applications-by-Class-of-applications |
| **Ch.** | Chapter |
| **CLRR** | 2017 European Parliament Resolution on Civil Law Rules on Robotics |
| **CSGD** | Consumer Sales and Guarantees Directive |
| **DCIR** | Draft Commission Implementing Regulation |
| **EC** | European Commission |
| **EG** | Expert Group |
| **EU** | European Union |
| **GPSD** | General Product Safety Directive |
| **G&BP** | Guidelines and Best Practices |
| **hEN** | Harmonized Standards |
| **HFT** | High-Frequency Trading |
| **IR** | Industrial Robots |
| **ISO** | International Organization for Standardization |
| **LLC** | Limited Liability Company |

| | |
|---|---|
| **MID** | Motor Insurance Directive |
| **MS** | Member States |
| **MTOM** | Maximum Take-Off Mass |
| **OECD** | Organisation for Economic Co-operation and Development |
| **PLD** | Product Liability Directive |
| **RCA** | Regulation (EU) 2018/1139 |
| **RMA** | Risk-Management Approach |
| **SAE** | Society of Automotive Engineers |
| **UA** | Unmanned Aircraft |
| **UK** | United Kingdom |
| **US** | United States |
| **WFD** | Framework Directive 89/391/EEC |

# LIST OF EXAMPLES



# LIST OF TABLES

# EXECUTIVE SUMMARY

***The need for technology-specific regulation of different AI-based solutions***

Regulating artificial intelligence requires defining it. Yet there is no consensus about what is to be understood by «AI».

The layman understanding of AI as machines and software with human-like capabilities and intelligence is far from accurate, and does not capture the reality of emerging technology. Indeed, only a small portion of AI-research pursues that objective («general AI»), and is decades away from achieving it, while the vast majority of research aims at developing specific solutions, with well-defined functions to be operated in given settings (light «AI»).

Indeed, when used for a different purpose or in a different setting, the same algorithm or application might radically change its nature as well as its social relevance, and thus lead to different regulatory needs. Facial recognition used to unlock a phone is not as problematic as when applied to mass surveillance.

Since AI is a heterogeneous phenomenon, its regulation cannot be single and unitary, not even with respect to liability rules. Any attempt to regulate AI needs to be technology-specific.

This is best understood by looking at how AI is pervasive. Already today, and even more in the future, it will be used in the most diverse fields of application, ranging – but not limited to – consultancy (in the financial, legal and medical sector), consumer products and services, mobility, online connectivity (including through platforms), energy production and distribution (e.g.: smart grids), cure of frail individuals (elderly, children, people with disability), policing and justice administration, to name a few. All those fields are separately regulated both by member states and the European Union – when relevant –, most typically even with respect to liability rules. Indeed, medical malpractice, professional responsibility, intermediaries' liability, liability for things in custody, for high-risk activities, for the acts of children, circulation of vehicles, nuclear energy production, are all separately addressed.

Why the advent of AI should change such a consolidated approach does not appear evident *per se*, in particular when considering how there appears to be no clear unifying trait of said AI-based applications.

***AI-based applications as products and the issue of legal personhood***

As of today, the only possible fundamental and universal consideration about AI-systems, is that there is no philosophical, technological nor legal ground to consider them anything else but artefacts generated by human intellect, and thence products.

From an ontological perspective, all advanced technologies are not subjects, but merely objects, and there are no reasons to grant them rights, nor hold them legally responsible. Even in light of existing liability rules it is always theoretically possible to identify a human being who might be deemed responsible for damages arising from the use of the device. In this sense, the liability framework may be suboptimal – e.g. because it gives rise to high-cost and complex litigation – , but excludes the existence of a responsibility gap.

From a functional perspective, on the contrary, we may identify some conditions under which it could be appropriate to attribute a fictitious form of legal personality to a specific class of applications, as it is today done with corporations. Such conditions consist in the need to (i) pursue coordination among multiple parties, for instance when multiple subjects are involved in providing an AI-based service or product and isolating the responsibility of each might prove hard, if not impossible; (ii) separate assets and limit responsibility, to ease both the distribution of the revenues as well as the apportionment of the damages generated from the technology; (iii) pursue transparency through registration and disclosure duties, to identify those parties who bear an economic or other interest in the functioning of the device; (iv) impose different – more or less favourable – levels of taxation, eventually also to incentivize the development of those products and services that are deemed more desirable.

Attributing legal personality is not the only way of achieving this effects. For most of, if not all, existing applications, resorting to other legal tools is indeed preferable (see Ch. 4 below). However, there are not technical grounds for radically excluding the possibility to grant legal personality to specific classes of AI-systems in the future, nor doing so would entail attributing the machine rights and duties equivalent to that of a natural person, or even of a slave.

### *Fault-based and contractual liability rules*

The existing legal framework at MS's level, primarily resting upon fault-based (or *culpa aquiliana*) and contractual liability rules is therefore applicable to all advanced technologies.

Fault-based liability, which is common to all MS's despite presenting some degrees of variation, establishes the duty to compensate damages upon the subject who negligently failed to maintain a desired standard of behaviour, causing damages. Vicarious liability and other forms of indirect liability rules – for things or animals in custody, or for the acts of children and auxiliaries – could be applied, holding primarily owners, and users of advanced technologies liable.

Contractual liability, instead, presupposes a legally qualified relationship (contract or legal obligation) between the parties before damage occurs. Said rules are also common to all MS's and are typically deemed more favourable to the claimant than fault based ones. They could apply holding the seller or service provider liable, whenever a pre-existing duty (to perform or protect) is identified.

Yet such rules might prove burdensome for the claimant – *culpa aquiliana* – or anyway hard to apply – absent a specific legal relationship between the parties – overall discouraging access to justice – due to technological complexity – and therefore lowering trust in technology, and its subsequent uptake. Differences among MS could also lead, in some cases, to market fragmentation. Their adequacy, however, is best assessed through a bottom-up, class-of-application-by-class-of-application analysis, of the kind described under the Risk-Management Approach below, taking into account the specificities of the given technology.

### *The European legal framework*

Since AI-based applications are to be deemed objects and products, with respect to the EU legal framework they primarily fall under two different bodies of legislation, (i) product safety regulation and the (ii) product liability directive (PLD). While the first set of rules imposes essential safety requirements for products to be certified and thus distributed onto the market, the latter aims at compensating victims for the harm suffered from the use of defective good, namely, a product that lacks the level of safety that it would be reasonable to expect.

The first body of norms is essential and plays a great role in ensuring the safety of users and consumers within the European market. Its potential – through *ex ante* detailed regulation and technical standardization – could be further exploited, favouring the development of narrow tailored and appropriate norms for emerging technologies, also in those fields where, currently, they are under developed.

The PLD has recently been assessed and found to be «coherent with the EU legislation protecting consumers, relevant and future-proof» and «fit for purpose»[1] However, commentators believe that many aspects should be revised, in particular – yet not exclusively – to ease its application to advanced technologies, in light of their complexity and opacity.

On more general grounds, the directive is also criticized for failing to achieve high levels of harmonization among MS, who still resort to other bodies of norms – in contracts and torts – to address defective products, and at times possess ad-hoc legislation for some categories of products – such as pharmaceuticals – leading to different outcomes in different European jurisdictions.

Indeed, a reform of the PLD is advisable, yet not sufficient to successfully address the regulation of AI-based technologies at European level. In particular, the PLD is based on a technology neutrality principle, whereby that piece of legislation should be equally applicable to any kind of product.

Yet, the simple empirical observations of the case litigated across European MSs shows an evident clustering around those products that are either technologically simple (raw materials), or cause relevant harm – in terms of damage quantification, number of people involved, and nature of the interests affected (e.g. bodily integrity and health), such as for pharmaceutical products – or that might be litigated by more sophisticated parties – businesses rather than consumers –.

Since the PLD is used only in cases which provide adequate incentives to face complex and costly litigation on the side of the victim, its theoretically broad scope of application is not reflected in every day practice. In particular, smaller-value claims where damage is suffered as a consequence of the failure of a product – that are certainly going to increase in number over time, the more automation diffuses, absent a human agent, in providing goods, services, and undergoing activities (e.g.: driving) – are not effectively addressed by the PLD.

Thus, we should not consider the PLD as truly technology neutral.

### *A European approach to regulating civil liability of AI*

Technology regulation should occur at EU level to achieve the maximum level of possible harmonization among MS. To this end, regulations rather than directives could prove a preferable tool in most cases.

Indeed, liability rules – shaping incentives for all parties involved in the research, development, distribution and use of a given technology – influence what kind of technology – and among multiple alternatives, solution – prevails. Different liability rules could therefore provide correspondingly divergent incentives for products to be distributed in each MS, leading to market fragmentation, hampering competition, and ultimately negatively affecting European industries.

Moreover, although national legal systems offer solutions for compensating victims of advanced technologies, the latter might prove excessively burdensome. Apportioning liability among multiple potential responsible parties will become increasingly difficult due to the overlap of different body of norms – including the PLD –, as well as to the opacity and complexity of many AI-based applications. Ascertaining a clear causal nexus between a given conduct and the harm suffered by the victim will become ever more complex and costly, if not impossible, potentially giving rise to «alternative causation» scenarios, and will frequently prevent the victim from achieving compensation. This, in turn,

[1] European Commission (2018). Report from The Commission to the European Parliament, the Council and the European Economic and Social Committee on the Application of the Council Directive on the approximation of the laws, regulations, and administrative provisions of the Member States concerning liability for defective products (85/374/EEC). Brussels, European Commission., 34 and 70.

would diminish users' trust in advanced technologies, delaying their uptake, and ultimately damaging European industry.

In such a perspective, the principle of functional equivalence should not induce policy-makers to replicate approaches elaborated over time by legislation, doctrinal research and case law. On the contrary, it should go beyond them, and adopt solutions rooted in substantial norms over those that primarily rely on civil procedure, also for reasons of more effective harmonization among MS.

Finally, and above all, proposed solutions cannot be technology neutral.

The use of AI is not a unifying trait, allowing for the separation of a given *Fallgrupp* that might be regulated unitarily. Quite the contrary, it is such a heterogeneous phenomenon that it might only be understood, and thence regulated, taking its diversity – and the diversity of approaches it encompasses – into account.

If medical malpractice and road accidents are today regulated through distinct liability rules, the fact that AI will be used in both sectors does not suggest they should be addressed unitarily in the future. Indeed, those MS that have today made efforts towards regulating some kinds of advanced applications – e.g.: drones and driverless vehicles – have done so with separate regulation, emphasising their peculiarities, an adopting norms rooted in the technical elements characterizing each one of them.

Distinctions based on the anticipated risk of given technologies are thus insufficient and unnecessary.

On the one hand, there is no data for calculating the «significance» of harm – as a function of its severity and frequency –, since the very risks posed by advanced technologies are hard to map. On the other hand, the criteria selected to assess severity are criticisable – an expert system for medical diagnosis does not necessarily pose less risks than a driverless car – and incomplete, since they do not take into account market failures and the overall efficiency of the legal system specifically applicable to the given technology.

Furthermore, only those technologies that truly pose societal concerns give rise to relevant risks, and represent a new potential that is not well framed within the current legal system, should be specifically addressed, through ad hoc regulation. In recent years, the EU has regulated drones, and platforms – for which it is considering revising its legislation – separately. In the future, it should continue to do so, more closely monitoring emerging technologies – eventually through a dedicated agency or group of experts – to identify those fields that require prompt intervention. Efforts in technology regulation at European level should overall increase, but they should be tackled through dedicated acts, when necessary, and a number of fields may already today be identified, that would deserve attentive consideration (see also Ch. 5 below). How, and on the basis of which criteria the need for normative intervention is appraised, depends on a number of elements that vary for the single class of applications.

Therefore, while normative intervention in the field of technology regulation is of the highest strategic importance at EU level, it should not be generalized and should be minimally invasive in all non-strictly relevant cases, according to the principle of proportionality and subsidiarity.

When relevant, the rationale behind reform should be that of imposing liability on the party who is in control of a given risk and can successfully manage it. Such a functional reasoning, also implied by the EG, should be applied on a class-of-applications-by-class-of-applications (CbC) basis, as defined by the so called Risk-Management Approach (RMA).

***A Risk-Management Approach to the civil liability of AI-based applications: theoretical and methodological considerations***

The RMA attributes liability to the party that is best positioned to (i) identify a risk, (ii) control and minimize it, and (iii) manage it – ideally pooling and distributing it among all other parties – eventually through insurance, and/or no-fault compensation funds. To do so, it resorts to strict – if not absolute – liability rules.

Indeed, the RMA does not attempt to incentivize compliance with an intended conduct – e.g. development of safe products –, as empirical considerations prove that adequate *ex ante* deterrence is often best achieved through other market or regulatory tools, such as reputation and *ex ante* product safety rules.

Liability rules should primarily aim at ensuring victim's compensation. Indeed, failures in the legal system might prevent victims from receiving the deserved compensation, allowing the parties that benefit from an activity to externalize social costs, leading to distortive effects in the market and competition.

A RMA is essential when the risk of undercompensating victims is a serious concern, as it happens with advanced AI-based applications, where victims find it difficult and costly to identify the relevant causal factor behind the damage, due to the opacity and complexity of the systems and the interaction of multiple parties in providing a good or service, which causes different liability regimes to overlap.

Victims facing too high litigation costs would either not sue – and bear themselves the negative consequence of the accident – or sue the weaker party– possibly another user of private owner of the technology, e.g.: the owner of a driverless car – in any case preventing an appropriate internalization of costs by those that control the risks and benefit from them.

To favour access to justice, and avoid «alternative causation» scenarios, it is essential to clearly identify the party who, *prima facie*, should be called in to compensate the damage, leaving further distribution of those costs among the subjects involved to price mechanisms, secondary litigation, and contractual agreements.

This problem is therefore best addressed by identifying *ex ante* a single, clear and unquestionable, entry point for all litigation, according to a one-stop-shop approach. Therefore, among the possible parties that could benefit from the use of a technology, and who are in the position to identify and control risks, one should be selected, who is held responsible towards the victim on strict – if not absolute – grounds.

This party will vary according to the different kinds of technological applications considered, in light of their complexity and functioning, as well as the way incentives are shaped. (see Ch. 3, and Ch. 5 below).

The party who is first called in to compensate damages is not necessarily the one who ultimately bears the cost of the accident. Indeed, market mechanisms – above all price – allow the burdened party to estimate the cost of liability – insurance transforms *ex post* uncertainty into a defined *ex ante* cost – and distribute it to all users, who benefit from a product or service. Moreover, rights to act in recourse – in secondary litigation – as well as contractual agreements allow him to distribute the costs along the entire value chain, burdening to the party that is specifically in control of the one risk that materialized.

Such a solution would minimize first level litigation between the victim and the sole clearly responsible party, to the advantage of the former, and of the legal system overall – preventing excessive burden for the MS' and European court system – as well as for the industry.

Such mechanism is not foreign to European law. Indeed, it is embodied by the Consumer Sales and Guarantees Directive (CSGD), that contributed to the effective consumers' protection, since consumers who receive non-conforming goods (art. 2 CSGD) are entitled to act directly against the seller, even if it is clear that he has no direct control over product quality (art. 3 CSGD), without resorting to complex litigation.

This positive experience offers a potential model for the regulation of advanced and AI-based technologies.

Alternatively, when multiple parties contribute to providing a complex and opaque AI-based product or service, and disentangling their roles might appear ever more difficult, as well as identifying the optimal entry point for litigation, the creation of a legal or electronic person might serve the identical purpose. A similar approach might be preferable for AI-based services – non-embedded AI solutions used in consultancy or to operate on capital markets – rather than AI- based products, such as driverless cars –. Indeed, the new legal entity would see the participation of all the different parties involved in providing the service, who ultimately would bear the costs of liability according to their share of interest in the entity itself.

Finally, to make higher risks more manageable, different approaches might be used, including first- or third-party compulsory insurance, automatic no-fault compensation funds, and liability caps either on their own or in combination with one another.

Compulsory insurance is not always an ideal solution. Absent adequate of statistically relevant data, risks might be hard to define and assess, and a generalized duty to insure might have a strong technology chilling effect. Automatic compensation funds – financed through ad-hoc taxes/fees imposed on the (i) producers, and/or (ii) service providers, and/or (iii) users of product or service or through public spending – typically coupled with damage caps and limitations could be considered in some of such cases. Damage caps and limitations, if provided, should be proportionate to the specific risks a given class of applications gives rise to, that might typically differ from those triggered by a different one.

Those criteria ought to be applied to sufficiently defined and uniform classes of technological applications, once the applicable legal framework is assessed, and the need for specific legal intervention observed.

### *Case studies*

Applying this rationale to some relevant technological fields allows some conclusions to be drawn.

While industrial robots appear overall well-regulated – ensuring an easy point of access for all litigation by the victim – connected and automated vehicles would benefit from a normative intervention at EU level to simplify the complex scenario that emerges from the multiplication of potential responsible parties, and to avoid legal and market fragmentation among MS. Drones are also adequately framed, however, an effort to harmonize liability among MS's legislation – privileging the responsibility of the operator – might prove useful, despite less pressing than for driverless cars.

AI-based applications in medical diagnosis, instead, require attentive consideration. On the one hand, they represent relevant opportunities to improve medical care, and yet the current liability framework could excessively burden medical practitioners. Shielding doctors from excessive litigation, and introducing alternative solutions for victim compensation (including forms of enterprise liability) should be prioritized.

# 1. THE DEFINITION OF AI, AND ITS CLASSIFICATION UNDERSTANDING COMPLEXITY

**Impossibility of elaborating a complete, all-encompassing, general definition of AI.**

1. Artificial intelligence (AI) is a buzzword, conceptualized as having one clearly identified meaning, and referring to a single entity to be addressed unitarily [§ 1].
2. However, that of AI is actually a vague and indeterminate concept, covering a vast, heterogeneous, and constantly evolving series of applications [§ 1].
3. The general public considers AI as a branch of studies that aims to create machines or programs possessing human-like qualities [§ 1].
4. AI applications, instead, more commonly pursue a specific function or use (driving, analysing data, controlling a smart-home environment), that is not related to human capacities (so called «light AI»). Only a limited part of AI-related research aims at replicating human-like capabilities (so called general «AI»). [§ 1.2].
5. In the technical debate, there is no consensus on a viable definition of AI. The characteristics of a given AI-application are defined by (i) the functions it pursues, and the (ii) environment it operates in. The resulting spectrum of applications is broad and diversified, with limited commonalities [§ 1.3].
6. AI is pervasive: its applications evolve and penetrate the most diverse fields of human activities [§ 1.3].
7. AI is a moving target: what is deemed an AI application is no longer considered as such when technology advances [§ 1.3].
8. In the policy making debate, various criteria are inconsistently used to define AI [§ 1.4].
9. In the US, policy documents acknowledge the impossibility of defining AI unitarily, and refer to specific solutions and systems, regardless of whether they are considered AI solutions or not [§ 1.4].

**Rejection of technological neutrality. Need for a bottom up, class-of-application-by-class-of-application (CbC) approach.**

10. Different AI-based applications give rise to different social, legal, ethical and economic concerns, according to the purpose for which, and the setting where they are used in [§ 1.5].
11. The idea of a technology-neutral and general AI regulation shall be rejected, in favour of a bottom-up, class-of-application-by-class-of-application legislative approach (CbC) [§ 1.5].
12. A CbC approach is more coherent with the one adopted as of today in regulating technology, at EU and MS level [§ 1.5].

## 1.1. Seeking a definition of Artificial Intelligence

Artificial Intelligence (henceforth "AI") is a term that is commonly used by policy makers when presenting their strategies on the governance of technological developments and the associated economic and social challenges, by companies that advertise products displaying some degree of automation, and by the media when presenting to the general public their comments on the so-called fourth industrial revolution. Sometimes AI literacy is even presented as a new skill for the future of work.

Ultimately, AI is a new buzz word. Indeed, AI is being conceptualized by the general public and policy makers alike as one broad umbrella notion, creating the impression that there is only one entity – AI –, that can be tackled unitarily, and eventually regulated as such.

However, looking closer at the technologies being developed, and classified as AI applications, this perception of unity is soon doomed to vanish. There are indeed very diverse devices that might be deemed AI-based or AI-operated systems, so diverse from one another as a driverless car, a smart-toothbrush, a robot-companion, a non-embedded expert system for medical diagnosis.

In a policy making perspective, clearly identifying the object to be regulated is not simply of paramount importance but strictly necessary. Absent a precise definition, the scope of the intended regulation will be uncertain, being either over- or under-inclusive, and triggering litigation. In such a sensitive field of technological innovation, this uncertainty might also hamper the very development of desirable technologies, and ultimately harm the market that well-conceived normative intervention otherwise aims to foster.

A correct understanding of this notion is also necessary to help the general public to correctly understand what these technologies entail, what they might bring about, how they might affect – when they could – our ways of life, and our rights. On the one hand, this defies dystopic science-fiction based accounts that lower trust in technology, delaying its uptake even when desirable; on the other hand, it favours an aware debate on those issues that are, instead, most sensitive for they touch upon core values and fundamental rights of the individual.

Therefore, even if the scope of this study is that of addressing the very specific issue of the – optimal – civil liability regulation for AI-based technologies, the first logical step is that of addressing the very definition of AI, to determine whether it is actually possible to conceive it unitarily and regulate it as such or, instead, whether a technology-specific, Class-of-applications-by-Class-of-applications approach (henceforth “CbC”), is preferable, if not altogether necessary.

For this reason, the study will first present an overview of the general definitions and main resources of AI, typically referred to in the non-technical debate, selected from prominent dictionaries (see § 1.2 below). This, indeed, represents a sufficient proxy of the general public’s perception of this phenomenon.

Then, it will take into account the technical debate, providing a necessarily incomplete yet representative overview of the scientific literature and determine whether there is a consensus on what falls within the notion of AI, and, eventually, what criteria enable an objective selection of applications that ought to be framed under this notion (see § 1.3 below ). This second step will serve the twofold purpose of (i) determining what AI is, *stricto sensu*, and (ii) assess whether this is commensurate to what policy makers typically refer to, when discussing AI-regulation.

Finally, definitions adopted by policy makers will be considered, with a more prominent – yet not exclusive – focus at EU level (see § 1.41.4 below).

The analysis will show that there is no single notion of AI and that the criteria commonly used to qualify certain categories of AI applications are broad and often indeterminate, and, thus, inadequate as a basis for adopting clear and effective regulation (see § 1.5 below).

Indeed, regulation cannot be technology neutral, since it is intrinsically tied to its scope and object, and thus it needs to take into account specific features of each technology. Against this background, it is indeed necessary to elaborate granular and narrow tailored classifications, distinguishing AI applications into different classes of devices.

## 1.2. Non-technical definitions of AI

Dictionary definitions have neither regulatory, nor scientific value. Yet, they depict and closely represent the social perception of a complex and multifaceted phenomena such as AI, which policy makers refer to, when deciding to intervene.

Therefore, before considering strictly technical definitions (see § 1.3 below), examples derived from prominent dictionaries need to be taken into account, and briefly discussed as a viable approximation of the layman's understanding of the subject matter.

The selection – which necessarily incomplete – is based on online resources.

### Table 1 - Non-technical definitions of AI

| Dictionary | Merriam Webster Dictionary | FranceTerme | Diccionario de la lengua española | Treccani | Wikipedia.de |
|---|---|---|---|---|---|
| Definition | «a branch of computer science dealing with the simulation of intelligent behavior in computers; 2: the capability of a machine to imitate intelligent human behaviour»[2]. | «Champ interdisciplinaire théorique et pratique qui a pour objet la compréhension de mécanismes de la cognition et de la réflexion, et leur imitation par un dispositif matériel et logiciel, à des fins d'assistance ou de substitution à des activités humaines»[3]. | «Disciplina científica que se ocupa de crear programas informáticos que ejecutan operaciones comparables a las que realiza la mente humana, como el aprendizaje o el razonamiento lógico»[4]. | «riproduzione parziale dell'attività intellettuale propria dell'uomo (con partic. riguardo ai processi di apprendimento, di riconoscimento, di scelta) realizzata o attraverso l'elaborazione di modelli ideali, o, concretamente, con la messa a punto di macchine che utilizzano per lo più a tale fine elaboratori elettronici (per questo detti cervelli elettronici)»[5]. | «Teilgebiet der Informatik, welches sich mit der Automatisierung intelligenten Verhaltens und dem maschinellen Lernen befasst. Der Begriff ist insofern nicht eindeutig abgrenzbar, als es bereits an einer genauen Definition von „Intelligenz" mangelt»[6]. |

[2] See https://www.merriam-webster.com/dictionary/artificial%20intelligence (last accessed June 29th 2020).
[3] See http://www.culture.fr/franceterme/terme/INFO948 (last accessed June 29th 2020).
[4] See https://dle.rae.es/inteligencia?m=form#2DxmhCT (last accessed June 29th 2020).
[5] See http://treccani.it/vocabolario/intelligenza/ (last accessed June 29th 2020).
[6] See https://de.wikipedia.org/wiki/Künstliche_Intelligenz (last accessed June 29th 2020).

First, all of the above definitions converge in considering as «AI» machines and/or computer programs that possess human-like capabilities or intelligence. This, however, is far from accurate. Indeed, no machine or software displays human-like intelligence, nor research primarily pursues this end, typically favouring the development of a specific and task-oriented capability (so called «light-AI»)[7] that often times exceeds what would be – if at all existing – the equivalent human performance (see § 1.3.1 below).

Second, the definitions sometimes enumerate those human traits that an AI-system should possess, such as visual perception, speech recognition, translation between languages and decision-making. Once again, this is not correct: as further explained below (see § 1.3.2 below) these are in fact functions enabled by resorting to different and not qualifying features, holistically displayed by one, single AI entity.

Said otherwise, AI is being explained by reference to some of its applications and by their replication of human capacities. On the one hand, this shows that, even in the simplest terms, understanding AI requires focusing on its specific applications. Only by abiding a granular approach it is possible to achieve the level of accuracy, necessary to understand the technology, the issues it might give rise to, and ultimately the domains that require regulation (see Ch. 5, § 5.1, § 5.2, and § 5.3). On the other hand, it is apparent that the very *prémisse majeure* used for defining AI – i.e. the existence of human-like intelligence – incorrectly narrows the scope of the definitions, since many existing AI-based applications are not related to it.

## 1.3. AI in the technical literature

The fundamentals of the concept of intelligent machines are set in Alan Turing's essay, *Computing Machinery and Intelligence,* whereby it is envisioned that computers may simulate intelligence similar to that of humans, assessed on a test evaluating natural language conversations between the machine and a human. However, the term artificial intelligence was actually first coined by John MCarthy who invited a group of researchers to participate at the first AI conference in 1956 at Dartmouth Summer Research Project on Artificial Intelligence, with the aim of investigating «ways in which machines could be made to simulate aspects of intelligence»[8]. 50 years later, the same aim seems to be governing AI research with AI being defined as «the science and engineering of making intelligent machines, especially intelligent computer programs»[9].

In this sense, and as some of the dictionaries' definition referred above correctly state – «AI» is first and foremost a *science*, classified in a variety of subfields, whose general aim is that of creating intelligent machines.

However, and most importantly, scientists do not agree neither on what exactly constitutes the object of their studies – i.e., what intelligent machines actually are – (see § 1.3.1 below), nor on what the boundaries of their own disciplines are, both *vis a vis* other, connected disciplines (such as robotics and bio-engineering), and among the different subfields of AI studies (see §1.3.2 below).

[7] See Floridi, L. (1999). Philosophy and Computing: an Introduction, Routledge.

[8] Stone, P., R. Brooks, E. Brynjolfsson, R. Calo, O. Etzioni, G. Hager, J. Hirschberg, S. Kalyanakrishnan, E. Kamar, S. Kraus, K. Leyton-Brown, D. Parkes, W. Press, A. A. Saxenian, J. Shah, M. Tambe and A. Teller (2016). One Hundred Year Study on Artificial Intelligence (AI100). https://ai100.stanford.edu/sites/g/files/sbiybj9861/f/ai100report10032016fnl_singles.pdf, 50.

[9] McCarthy, J. (2007). WHAT IS ARTIFICIAL INTELLIGENCE? http://www-formal.stanford.edu/jmc/whatisai.pdf, 2 (last accessed June 29th 2020). Also, see Nilsson, N. (2010). The quest for artificial intelligence. A history of ideas and achievements, Cambridge University Press., 13, where AI is defined as «that activity devoted to making machines intelligent, and intelligence is that quality that enables an entity to function appropriately and with foresight in its environment».

This lack of a consensus on a viable definition among AI researchers has been widely recognized[10]. Quite curiously, it was even appraised, for «the lack of a precise, universally accepted definition of AI probably» has «helped the field to grow, blossom, and advance»[11].

### 1.3.1. AI for AI researchers

In the technical literature, a certain degree of consensus is reached on the very general understanding of intelligence, which is described as «the computational part of the ability to achieve goals in the world»[12], varying in kinds and degrees in people, animals as well as in some machines[13]. This definition, with some variations tends to be accepted among AI researchers[14].

All things considered, a machine or system is deemed intelligent when it can act in, adapt to, and learn from specific environments so as to achieve predefined goals. The specific manifestation given from the intersection of the function pursued and the environment it operates in, appear thence to be the qualifying elements of AI.

However, this definition is extremely general, and fails to give any technical information about the capacities that a system may display to act intelligently. This is because AI-systems can take many forms, which are influenced by at least two important and varying elements: (i) the environment where an AI-system is being used and (ii) the goal that it is set to achieve.

Thus, different environments and different goals can lead to manifold manifestations of the same software or system, and while a system can be seen as «intelligent» in one environment and towards a certain goal, it may be seen as «unintelligent» in a different scenario.

Furthermore, the ability of achieving goals can be benchmarked against various thresholds.

Indeed, it has been recognized that AI researchers cannot yet characterize in general what kinds of computational procedures they want to call intelligent[15], and when – given a certain procedure and task – the machine or software can be deemed sufficiently intelligent «to act in, adapt to, and learn from the specific environments to achieve a predefined goal».

Indeed, contrary to the layman's expectation, the benchmarks for assessing the system performance are varied, and not necessarily linked to the human capacities.

---

[10] Krafft, P. M., M. Young, M. Katell, K. Huang and G. Bugingo (2019). Defining AI in Policy versus Practice. Proceedings of the 2020 AAAI/ACM Conference on AI, Ethics, and Society (AIES). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431304, SSRN., 1. As recognized also by the US National Science and Technology Council Committee on Technology, «there is no single definition of AI that is universally accepted by practitioners»; see National Science and Technology Council Committee (2016). Preparing for the future of Artificial Intelligence. United States US Government, Office of Science and Technology Policy , 6.

[11] Agre, E. P. (1997). Lessons learned in trying to reform AI. Social Science, Technical Systems, and Cooperative Work: Beyond the Great Divide Psychology Press., 131.

[12] McCarthy, J. (2007). What is artificial intelligence? http://www-formal.stanford.edu/jmc/whatisai.pdf, (last accessed June 29th 2020), 2.

[13] Ibid.

[14] See in this sense the following authors defining "intelligence" as: «the ability of a system to act appropriately in an uncertain environment, where appropriate action is that which increases the probability of success, and success is the achievement of behavioral subgoals that support the system's ultimate goal» - Albus., J. S. (1991). "Outline for a theory of intelligence. ." EEE Trans. Systems, Man and Cybernetics 21(3): 473–509.; «Any system […] that generates adaptive behaviour to meet goals in a range of environments can be said to be intelligent» - Fogel, D. B. (1995). "Review of computational intelligence: Imitating life." Proc. of the IEEE 83(11).; «the successful (i.e., goal-achieving) performance of the system in a complicated environment» - Horst, J. (2002). A native intelligence metric for artificial systems. In Performance Metrics for Intelligent Systems Workshop. Gaithersburg, MD, USA.; «Intelligence is the ability to use optimally limited resources – including time – to achieve goals» -Kurzweil, R. (2000). The age of spiritual machines: When computers exceed human intelligence, Penguin.; «[An intelligent agent does what] is appropriate for its circumstances and its goal, it is flexible to changing environments and changing goals, it learns from experience, and it makes appropriate choices given perceptual limitations and finite computation» - Poole, D., A. Mackworth and R. Goebel (1998). Computational Intelligence: A logical approach. New York, NY, USA, Oxford University Press.; «Intelligence is the ability for an information processing system to adapt to its environment with insufficient knowledge and resources. - Wang, P. (1995). On the working definition of intelligence. Technical Report 94. Center for Research on Concepts and Cognition, Indiana University.

[15] McCarthy, J. (2007). What is artificial intelligence? http://www-formal.stanford.edu/jmc/whatisai.pdf, (last accessed June 29th 2020), 3.

This is further demonstrated by Stuart Russell and Peter Norvig, who – depending on the benchmark concretely used – present eight different definitions of AI used in the last 60 years by AI experts, which may be divided into (i) AI agents that think and act humanly and (ii) AI agents that think and act rationally[16]. In this sense, depending on the system at issue, its functions and predetermined goals, and the environment it operates in, something will qualify as AI only if success is measured «in terms of fidelity to *human* performance», whereas in other cases it will require «an *ideal* performance measure, called *rationality*»[17]. Thus, the same system, when benchmarked against the two thresholds, may be deemed as «intelligent» or not (e.g. while Web aggregators may be deemed intelligent based on the rational agent threshold, they may be not on the human intelligence one).

As the human intelligence threshold may often omit extant technologies that either don't reach said level of intelligence, or exceed it, Russell and Norvig generalize the second approach, and claim that AI is the science of designing rational agents whereas «a rational agent is one that acts so as to achieve the best outcome or, when there is uncertainty, the best expected outcome»[18]. Needless to say, what is the best expected outcome, will constantly vary, depending on technology state of the art, availability of data, desired outcomes, etc., and it is thus impossible to determine it in generalized terms.

This is indeed reflected in the continuous change and evolution of the meaning of AI, even within the technical discourse. AI suffers from the «AI effect» or the «odd paradox» where «AI brings a new technology into the common fold, people become accustomed to this technology, it stops being considered AI, and newer technology emerges»[19]. For example, spam filtering and language translation technology, although based on machine learning models, are not regarded by the public opinion, and neither by AI experts, as AI solutions worth debating on. Also, AI stays as the basis of the Internet as it is known today, since search engines, recommender systems, and Web site aggregators are created by using different AI techniques[20]. However, as such technology is becoming more ubiquitous, both to its users and to the experts building it, it loses the AI hype. Simply put, «[a]s soon as it works, no one calls it AI anymore»[21].

The above shows that striving to find a general definition for AI even in the technological field is a useless exercise.

Most importantly, such variations and indeterminacy in the procedures and the degree of performance which qualify a system as intelligent may seem unimportant in the technical field, and yet they are highly problematic in policy-making, where certainty about notions is required, to define the exact scope of regulation (see Ch. 3, § 3.5).

Indeed, as it will be shown, regulatory needs are not related to the intelligence of a system in itself, but rather to the social, legal and economic consequence that such intelligent systems have when deployed in society. In this sense, even if we were able, from a technical perspective, to reach a unique definition of AI – be it based on the human-like capabilities or the ideal ones of the rational agents – still said definition may not be deemed fit for regulatory purposes. For example, AI that plays chess and acts within the established parameters would be considered a rational agent, although there are no pressing cases that would require to regulate such an agent. On the contrary, many applications that

---

[16] Russell, S. J. and P. Norvig (2010). Artificial Intelligence. A Modern Approach, Prentice Hall., 2.

[17] Ibid., 1.

[18] Ibid., 4 and 59.

[19] Stone, P., R. Brooks, E. Brynjolfsson, R. Calo, O. Etzioni, G. Hager, J. Hirschberg, S. Kalyanakrishnan, E. Kamar, S. Kraus, K. Leyton-Brown, D. Parkes, W. Press, A. A. Saxenian, J. Shah, M. Tambe and A. Teller (2016). One Hundred Year Study on Artificial Intelligence (AI100). https://ai100.stanford.edu/sites/g/files/sbiybj9861/f/ai100report10032016fnl_singles.pdf, 12.

[20] Russell, S. J. and P. Norvig (2010). Artificial Intelligence. A Modern Approach, Prentice Hall., 26-27.

[21] Vardi, M. Y. (2012) "Artificial Intelligence: Past and Future." Communications of the ACM 55., 5.

fail to achieve the best expected outcome, would not qualify as rational agents and would fall outside the scope of any regulation that uses such notion (see in this respect § 1.4 and in particular the AI HLEG's definition of AI which uses the concept of the rational agent in defining AI-systems).

### 1.3.2. AI as a branch of computer science

An attempt to find a general definition for AI seems even more flawed, when looking at AI as «a branch of computer science that studies the properties of intelligence by synthesizing intelligence»[22]. This branch of computer science is comprised, currently, of many subfields, each with different characteristics with respect to what the resulting AI does, and how it does it, and what risks it poses.

Indeed, the following AI techniques have been identified in the science of AI: machine learning, probabilistic reasoning, logic programming, fuzzy logic and ontology engineering. Machine learning, which is the biggest AI subfield is further divided into: classification and regression trees, support vector machines, neural networks, deep learning, supervised learning, unsupervised learning, reinforced learning, etc[23].

All these techniques can have the following AI applications, each of them substantially different one from the other: computer vision (which is in turn divided into augmented reality, biometrics, object tracking, character recognition, scene understanding), robotics, natural language processing (divided into sentiment analysis, dialogues, semantics, natural language generation, machine translation, information extraction), planning and scheduling, predictive analysis, speech processing (speech recognition, speech synthesis, speaker recognition), etc[24].

However, the above AI applications are not only the result of alternative techniques (e.g. solely deep learning, or solely unsupervised learning ). They usually result from a complex combination of programming techniques intertwined, as well as on cognitive sciences. Thus, AI is a multiplex science of various and vast subfields which, when applied, may lead to various applications. Said variety, which is further exacerbated by different use cases of the same application, reflect that grasping all AI applications in a singular definition, let alone the entire concept of AI, is a faulty exercise lacking precision for the purpose of regulation.

Furthermore, machine learning and its applications are neither good, nor bad in essence. However, the manner in which these applications are being used can pose significant risks, such as computer vision being used for augmented reality or for studying customers' emotions in a shop.

Therefore, it is specific AI applications that should be the subject of regulation, and their specific use cases.

## 1.4. Notion of AI for policy-making/regulatory purposes

Regulating AI is a difficult task. Over-regulating AI could lead to a chilling effect on innovation, while under-regulating AI can lead to serious harms on the rights of citizens, as well as to losing an opportunity to shape the future of European society. Thus, «the stakes could not be higher» and «the way we approach AI will define the world we live in»[25]. While the world is trying to come to an

[22] Stone, P., R. Brooks, E. Brynjolfsson, R. Calo, O. Etzioni, G. Hager, J. Hirschberg, S. Kalyanakrishnan, E. Kamar, S. Kraus, K. Leyton-Brown, D. Parkes, W. Press, A. A. Saxenian, J. Shah, M. Tambe and A. Teller (2016). One Hundred Year Study on Artificial Intelligence (AI100). https://ai100.stanford.edu/sites/g/files/sbiybj9861/f/ai100report10032016fnl_singles.pdf, 13.

[23] (2019). WIPO Technology Trends 2019: Artificial Intelligence. Geneva, World Intellectual Property Organization., 24.

[24] Ibid., 26.

[25] Commission communication of 25 April 2018 on Artificial Intelligence for Europe COM(2018) 237 final. Brussels, European Commision., 1. Also see MS' Declaration of cooperation on Artificial Intelligence (AI) available at https://ec.europa.eu/digital-single-market/en/news/eu-member-states-sign-cooperate-artificial-intelligence (last accessed June 29th 2020) which states that the member states agree to cooperate

agreement, states, international organizations, non-governmental organizations and policy makers are working towards defining AI for the purpose of building an AI legal framework.

To this end, two approaches in defining AI have been identified. On the one hand, research groups such as the AI HLEG, national governments and international organizations strive for finding a general AI definition, and on the other hand, national legislators or political parties employ a more granular approach by passing or trying to pass laws that regulate specific AI applications.

This study presents fourteen definitions of AI used in governments' national strategies and policy papers. Although this collection is not meant to be exhaustive, it provides a broad picture on how AI is being perceived by national governments, international organizations and researchers.

These definitions, based on their content, have been assessed against seven criteria. Without being all-inclusive, the selected criteria cover the majority of the elements used in the definitions[26]. In the paragraph below, we identify each criterion, highlighting its importance and the effects of employing one or another on any strategy on regulating AI. They are «general» definitions, pertaining only to the first approach.

1. *Whether AI is a science, a system or functionality*. With respect to its effects on regulation, if AI is deemed a science that needs regulation, then the focus should be on regulating the integrity of its members, its organization, supervisory bodies, etc. If AI is a system that can be deployed in the real world which may have different impacts on our society, then regulation should be focused on how these systems are used, built, deployed and by whom. Therefore, the lens through which AI is being analysed will impact regulation.
2. *Whether AI can refer to both hardware and software systems*. Indeed, this distinction can have important effects on the harm that such a system may create (physical, moral and/or, non-pecuniary, pecuniary, and pure economic), thus requiring different rules.
3. *Whether there is a distinction between «weak» AI and «strong» AI or «narrow» AI and «general» AI*. This distinction is important because while the existing narrow AI directed at achieving specific tasks is being implemented, the general AI, which is one single system to work and perform tasks across different domains, still remains a desiderate and thus, policy papers focusing on future technologies and general AI will not solve existing problems raised by the technologies used today.
4. *Whether only the systems that are intelligent can be considered AI*. This, in turn, depends on how and whether intelligence is being assessed and explained, which is an important element given that, as shown above, intelligence is not an agreed upon term.
5. *Whether actual applications or future applications are being considered.* From a risk-management perspective, taking into account specific classes of applications is essential when regulating AI (see Ch. 5, §§ 5.1- 5.2).
6. *What types of functionalities shall systems display to be deemed AI*. Indeed, if a different understanding of AI may be unavoidable at global level, within the EU having different qualification of what constitutes AI can lead to a fragmentation of the European single market, and lead to substantial legal uncertainties. Therefore, if the functionality criterion is used for defining AI, consensus should be reached with respect to such functionalities.
7. *Whether definitions refer to AI research subfields, and which exactly.*

The outline of these definitions is presented in Table 2 below.

on «ensuring an adequate legal and ethical framework, building on EU fundamental rights and values, including privacy and protection of personal data, as well as principles as transparency and accountability».

[26] Please note that the criteria/elements of the definitions are not used in all definitions altogether, but all the definitions show that there is a pool of criteria from which policy makers choose from. This study aims at gathering all these scattered criteria/elements.

## Table 2 - Policy making definitions of AI

| General definitions of AI | Institution | Distinction between software/ hardware | AI is […] | Distinction between weak AI / strong AI | Intelligence | Applications | Features/ capabilities | Reference to AI research subfields |
|---|---|---|---|---|---|---|---|---|
| *«Artificial intelligence (AI) systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions. As a scientific discipline, AI includes several approaches and techniques, such as machine learning (of which deep learning and reinforcement learning are specific examples), machine reasoning (which includes planning, scheduling, knowledge representation and reasoning, search, and optimization), and robotics (which includes control, perception, sensors and actuators, as well as the integration of all other techniques into cyber-physical systems)»*[27]. | AI HLEG | Yes | - A scientific discipline;<br>-AI-systems are software and/or hardware systems | No | No; the definition uses the concept of rational agent | No | Yes<br>Reasoning<br>Learning<br>Acting and planning<br>Decision - making | Yes<br>Machine learning<br>Machine reasoning<br>Robotics |
| *«AI system: An AI system is a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy»*[28]. | OECD | No | AI-system/machine-based system | No | No | No | Yes<br>Autonomy<br>Decision-making<br>Planning | No |

[27] AI HLEG (2019). A definition of AI: main capabilities and disciplines, European Commission, Available at the following link https://ec.europa.eu/digital-single-market/en/news/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines

[28] OECD (2019). Recommendation of the Council on Artificial Intelligence, OECD. LEGAL/0449., 7.

| General definitions of AI | Institution | Distinction between software/ hardware | AI is […] | Distinction between weak AI / strong AI | Intelligence | Applications | Features/ capabilities | Reference to AI research subfields |
|---|---|---|---|---|---|---|---|---|
| *«interdisciplinary field, usually regarded as a branch of computer science, dealing with models and systems for the performance of functions generally associated with human intelligence, such as reasoning and learning»*[29] and *«capability of a functional unit to perform functions that are generally associated with human intelligence such as reasoning and learning»*[30]. | ISO | No | - An interdisciplinary field – branch of computer science<br>-The capability of a functional unit | No | Yes; human Intelligence | No | Yes<br>Reasoning and learning | No |
| *«Artificial intelligence is systems based on algorithms (mathematical formulae) that, by analysing and identifying patterns in data, can identify the most appropriate solution. The vast majority of these systems perform specific tasks in limited areas, e.g. control, prediction and guidance. The technology can be designed to adapt its behaviour by observing how the environment is influenced by previous actions. Artificial intelligence is used in a number of areas, e.g. search engines, voice and image recognition, or to support drones and -driving cars»*[31]. | Denmark national government | Yes<br>AI-systems used for digital applications and AI used to support drones and self-driving cars | Systems based on algorithms | No | No; definition refers to the notion of rational agent that can «identify the most appropriate solution». | Yes<br>Search engine<br>Voice and image recognition<br>Self-driving cars<br>Drones | Yes<br>Learning<br>Planning<br>Reasoning | No |

[29] ISO-IEC-2382-28 *self* * 1995 available at https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:ed-1:v1:en (last accessed June 29th 2020).

[30] ISO-IEC-2382-28 available at https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:ed-1:v1:en (last accessed June 29th 2020).

[31] (2019). National Strategy for Artificial Intelligence. B. a. F. A. Ministry of Finance and Ministry of Industry, The Danish Government., 6.

| General definitions of AI | Institution | Distinction between software/ hardware | AI is [...] | Distinction between weak AI / strong AI | Intelligence | Applications | Features/ capabilities | Reference to AI research subfields |
|---|---|---|---|---|---|---|---|---|
| *«AI can be defined as the Science and Engineering that allows the design and programming of machines capable of carrying out tasks that require intelligence. Rather than achieving general intelligence, current AI focuses on what is known as specific AI, which is producing very important results in many fields of application such as natural language processing or artificial vision; however, from a scientific and basic and applied research point of view, general AI remains the major objective to be achieved, that is, creating an ecosystem with intelligent multitasking systems»[32].* | Spain national government | No | AI is a science and engineering of design of intelligent machines | Yes | Yes, but it does not refer to human intelligence in particular. | Yes<br>Natural language processing<br>Artificial vision | No | No |
| *«"Strong" AI means that AI systems have the same intellectual capabilities as humans, or even exceed them. "Weak" AI is focused on the solution of specific problems using methods from mathematics and computer science, whereby the systems developed are capable of self-optimisation. To this end, aspects of human intelligence are mapped and formally described, and systems are designed to simulate and support human thinking. The Federal Government is oriented its strategy to the use of AI to solve specific problems, i. e. to the "weak" approach»[33].* | Germany national government | No | AI can be strong AI or weak AI | Yes | Yes, although human like capabilities are attached to strong AI only. | No | Problem-solving<br>Learning and self-optimizatio n | No |

[32] Ministerio de Ciencia, Innovación y Universidades (2019 ). Estrategia Española De I+D+I En Inteligencia Artificial I. y. U. Ministerio de Ciencia: 12.

[33] Germany, F. G. (2018). Artificial Intelligence Strategy: 4-5.

| General definitions of AI | Institution | Distinction between software/ hardware | AI is […] | Distinction between weak AI / strong AI | Intelligence | Applications | Features/ capabilities | Reference to AI research subfields |
|---|---|---|---|---|---|---|---|---|
| *«Artificial intelligence refers to devices, software and systems that are able to learn and to make decisions in almost the same manner as people. Artificial intelligence allows machines, devices, software, systems and services to function in a sensible way according to the task and situation at hand»*[34]. | Finland national government | Yes | AI refers to devices, software and systems | No | Yes, namely decision-making ability benchmarked against human capabilities. | No | Yes<br>Learning<br>Decision-making | No |
| *«Technologies with the ability to perform tasks that would otherwise require human intelligence, such as visual perception, speech recognition, and language translation»*[35]. | UK national government | No | AI refers to technologies | No | Yes<br>Criteria of performance is human intelligence. | Yes<br>Visual perception<br>Speech recognition<br>Language translation | No | No |

[34] Government, F. (2017). Finland's Age of Artificial Intelligence Ministry of Economic Affairs and Employment , 15.

[35] (2017). Industrial Strategy White Paper. H. Government. UK: 37.

| General definitions of AI | Institution | Distinction between software/ hardware | AI is […] | Distinction between weak AI / strong AI | Intelligence | Applications | Features/ capabilities | Reference to AI research subfields |
|---|---|---|---|---|---|---|---|---|
| *Although the* National Science and Technology Council Committee on Technology recognizes that the «diversity of AI problems and solutions, and the foundation of AI in human evaluation of the performance and accuracy of algorithms, makes it difficult to clearly define a bright-line distinction between what constitutes AI and what does not»[36], an AI definition is used and formulated by the US Defense Innovation Board, which defines AI as : «a variety of information processing techniques and technologies used to perform a goal-oriented task and the means to reason the pursuit of the task. When referring to the wider range of considerations, we use the term artificial intelligence (AI) ; however, where we specifically address machine learning (ML) systems, we refer to ML. Furthermore, we use the term AI systems to mean systems that have an AI component within an overall system or a system of systems»[37]. | United States | Yes, but implied, as AI systems mean systems that have an AI component within an overall system or a system of systems, which may include both hardware and software. | A variety of information processing techniques | No | No | No | Yes Reasoning | Yes Machine Learning |
| *«AI is a constellation of technologies that enable machines to act with higher levels of intelligence and emulate the human capabilities of sense, comprehend and act»[38].* | India national government | No | AI is a constellation of technologies | No | Yes Criteria of performance is human intelligence. | No | Yes Learning Acting Knowledge | No |

[36] National Science and Technology Council Committee (2016). Preparing for the future of Artificial Intelligence. United States US Government, Office of Science and Technology Policy , 7.

[37] Board, D. I. (2019). AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense. US, Department of Defense., 5. The Defense Innovation Board further clarifies that: «the 2018 DoD Strategy on AI defines AI to be: "the ability of machines to perform tasks that normally require human intelligence – for example, recognizing patterns, learning from experience, drawing conclusions, making predictions, or taking action – whether digitally or as the smart software behind autonomous physical systems." Our definition does not preclude the DoD AI Strategy's approach, but allows for a wider range of AI applications that do not require a human intelligence benchmark».

[38] (2018). National Strategy for Artificial Intelligence N. Aayog. India: 12.

| General definitions of AI | Institution | Distinction between software/ hardware | AI is […] | Distinction between weak AI / strong AI | Intelligence | Applications | Features/ capabilities | Reference to AI research subfields |
|---|---|---|---|---|---|---|---|---|
| *«artificial intelligence (AI) is the capability of a functional unit to perform functions that are generally associated with the human intelligence such as reasoning, learning and self-improvement. An AI system is a product, service, process or decision making methodology whose operation or outcomes is materially influenced by artificially intelligent functional units»*[39]. | UAE national government | Yes<br>AI-systems can be product, services or decision making methodologies | AI is the capability of a functional unit to perform tasks | No | Yes<br>Criteria of performance is human intelligence. | No | Yes<br>Reasoning<br>Learning<br>Self-improvement<br>Decision-making | No |
| *«"AIDA" refers to artificial intelligence or data analytics, which are defined as technologies that assist or replace human decision-making»*[40]. | Singapore national government | No | AI is a technology | No | No | No | Yes<br>Decision-making | No |
| *«The term "Artificial Intelligence (hereinafter AI)" […] presumes a system that realizes an intelligent function» and "although AI in recent years is mainly based on machine learning, especially deep learning, AI related technology is rapidly developing, and the definition of AI is not limited solely to technology used for AI»*[41]. | Japan national government | No | AI is a system that realizes an intelligent function | No | Yes, but it does not refer to human intelligence in particular. | No | No | Yes<br>Machine learning<br>Deep learning |

[39] (2019). AI Ethics principles & guidelines. S. Dubai. Dubai: 16.

[40] (2019). Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector. M. A. o. Singapore. Singapore: 5.

[41] Government, J. (2019). AI Strategy 2019 AI for Everyone: People, Industries, Regions and Governments (tentative translation）. T. a. I. Council for Science. Japan: 2-3.

| General definitions of AI | Institution | Distinction between software/ hardware | AI is [...] | Distinction between weak AI / strong AI | Intelligence | Applications | Features/ capabilities | Reference to AI research subfields |
|---|---|---|---|---|---|---|---|---|
| *«A collection of interrelated technologies used to solve problems autonomously and perform tasks to achieve defined objectives without explicit guidance from a human being». «This definition of AI encompasses both recent, powerful advances in AI such as neural nets and deep learning, as well as less sophisticated but still important applications with significant impacts on people, such as automated decision systems." The categorisation between "narrow" and "general" AI is mentioned. The "narrow AI" performs specific functions. The "general AI" "is comparable to human intelligence across a range of fields»*[42]. | Australia national government | No | AI is a collection of interrelated technologies | Yes «narrow AI» and «general AI» | Yes, although human like capabilities are attached to general AI only. | Yes Automated decision systems | Yes Autonomy | Yes Neural nets Deep learning |

[42] Dawson, D., E. Schleiger, J. Horton, J. McLaughlin, C. Robinson, G. Quezada, J. Scowcroft and S. Hajkowicz (2019). Artificial Intelligence, Australia's Ethics Framework. A Discussion Paper. Australia: 14.

Four of the definitions refer to AI as «technologies», while others – such as that of the AI HLEG – refer to it as both a science and systems, while others consider it the capability of a functional unit to perform certain tasks. While this is accurate in essence because it grasps the two semantic meanings of the term «AI», it is debatable how focusing on defining AI as a science will serve the purpose of regulation. If such a definition were to be used to regulate rights, obligations and liabilities, the broad scope of application of this notion would most likely make the regulation over-inclusive. At the same time, it would be under-inclusive, as the definitions that refer to AI as a science only exemplify a couple of its subfields such as neural nets, machine learning, deep learning and robotics, neglecting others, such as classification and regression trees, support vector machines, supervised learning, unsupervised learning and reinforced learning.

Furthermore, only some of the definitions distinguish between strong AI vs. weak AI. These definitions acknowledge that there is no general AI to be applied across multiple sectors. This is an important acknowledgement as it shows a focus on existing technologies rather than on future ones. Although not all definitions make this express distinction, the majority of the definitions refer to AI-systems as algorithms that are programmed to achieve only specific tasks and solve specific problems, which is an implicit acknowledgement of the existing narrow or light AI. At the same time, defining AI as a system designed to achieve certain goals and perform specific tasks in a given environment will lead to a broad and vague definition. As shown in § 1.3, different environments and different goals can lead to many manifestations of the same software or system. Thus, given the acknowledgement that AI cannot be generally defined, but that there are many clusters of AI types and systems, the focus in defining AI should be on specific technologies and applications that act in well-identified environments and for given goals.

Moreover, the majority of the definitions refer to AI as systems or methodologies that are «intelligent». This concept used by AI experts, has been transplanted to policy-making, although, as presented above in § 1.3, intelligence is a divergent concept even in the technological and engineering world. While some of the definitions refer to AI as systems that perform tasks usually associated with human intelligence, the AI HLEG employs instead the definition of the rational agent, referring to AI as a system designed to achieve the best outcome. Both approaches are susceptible to criticism. First, as mentioned in § 1.3.1, defining AI as human-like intelligent systems is an under-inclusive manner of defining AI as it leaves out other AI technologies which don't mirror human-like capabilities. Second, defining AI-systems as rational agents that take «the best action» or «best expected action» is both over-inclusive and under-inclusive. It is over-inclusive because not all AI applications that achieve the best outcome require regulation, such as a chess playing software. Also, it is under-inclusive because if AI is a software that acts and decides on the best action(s) to take to achieve the given goal, any software programmed to decide to take any action other than «the best one» (which nevertheless is a very vague term) or one that would fail to decide which is such best action, would fall outside the scope of regulation. Thus, any agent acting irrationally would not be subject to a law defining AI as a rational agent, although an irrational agent is more likely to create harm than a rational one.

Furthermore, only four definitions acknowledge that AI-systems can be hardware and/or software based, although such a distinction bears important significance with respect to regulation.

Last but not the least, the majority of the definitions refer also to AI functionalities and capabilities, but these very much vary as it can be seen from Table 2. Reasoning, learning, self-improvement, autonomy, decision-making, planning and problem solving were identified as capabilities used to define AI-systems, but these capabilities are not equally recalled in all definitions leading to alternative classifications of the identical technological solution. Uniformity among MS in this respect is essential to avoid market fragmentation, and hard to overcome future path-dependencies.

## 1.5. Discussions and conclusions

The above findings show that the both generic, technical and policy-making definitions are lacking precision in identifying the borders of this complex field. Differences among research branches, notions, and ultimately applications are so relevant that renouncing at elaborating a general definition seems advisable. The same is concluded in the United States by the National Science and Technology Council Committee on Technology, by stating that:

> «This diversity of AI problems and solutions, and the foundation of AI in human evaluation of the performance and accuracy of algorithms, makes it difficult to clearly define a bright-line distinction between what constitutes AI and what does not»[43].

Rather than starting from the general, while leaving out specific but disruptive technologies, regulators should strive to find specific definitions which could prove useful to address narrowly identified problems posed by AI applications. Specific regulation cannot be avoided anyway, because generalizing a concept or field directly involves eliminating features or capabilities, either present or future, which most likely will require an attentive assessment and possibly normative intervention.

Furthermore, technologies pose different risks depending on their use. For example, facial recognition technology may be harmless if it's used by consumers to unlock their smartphones, but it can pose substantial risks and human rights concerns if used for mass surveillance. Moreover, AI technology embedded in hardware that can physically interact with the environment will pose different risks than non-embedded applications, each with its own peculiarities. Therefore, there is a need for a «sector-specific approach that does not prioritize the technology, but focuses on its application within a given domain»[44], tackling the most pressing and stringent concerns technologies pose today.

Such an approach was already suggested as preferred by early studies in technology regulation[45].

Moreover, regulation is an effort primarily aimed at determining how an observed phenomenon ought to be framed within society, in order to power its development. This entails focusing on the social implications of a given function and technology.

This also entails stating that a given technological trait or function only matters, in a regulatory perspective, for the way it impacts our social and economic structure and the rights and values it is based upon. Said otherwise, a ground-breaking technological solution might not give rise to social concerns or opportunities as much as another that, despite less innovative, squarely affects and conflicts with fundamental values and rights[46].

Finally, the attempt to deliver future-proof definitions and all-encompassing regulations is empirically flawed. A broad regulatory approach, attempting to include all existing and even not directly foreseeable uses of AI, would be doomed to being both incomplete and ineffective.

---

[43] National Science and Technology Council Committee (2016). Preparing for the future of Artificial Intelligence. United States US Government, Office of Science and Technology Policy , 7.

[44] Whittaker, M., K. Crawford, R. Dobbe, G. Fried, E. Kaziunas, V. Mathur, S. Myers West, R. Richardson and J. Schultz (2018). AI Now Report 2018, AI Now Institute, New York University: 8.

[45] Bertolini, A. (2013). "Robots as Products: The Case for a Realistic Analysis of Robotic Applications and Liability Rules." Law Innovation and Technology 5(2): 214, Bertolini, A. and E. Palmerini (2014). Regulating Robotics: a Challenge for Europe. Upcoming Issues of EU Law, available at http://www.europarl.europa.eu/document/activities/cont/201409/20140924ATT89662/20140924ATT89662EN.pdf. D.-G. f. I. Policies. Bruxelles., 180-182.

[46] For example, on the one hand recommender systems and web aggregators nowadays pose significant risks when used for voting manipulation and providing access only to some news and information and not to others which are automatically deemed by the algorithm as not being of interest by the user. These algorithms may pose significant risk for democracy and citizens' right to access to information. On the other hand, speech recognition and language understanding based systems used for building chatbots, albeit being new technology with respect to which we can even affirm that it emulates human-like capabilities, do not pose a significant risk when used for their intended purpose.

Incomplete, because it would be under-inclusive of some developments that might occur and still be hard to frame within the provided definitions.

Ineffective, because to be sufficiently generic it may not adequately focus on those peculiarities that give rise to relevant concerns and opportunities for society.

Therefore, regulation cannot be technology neutral since it aims at governing the social changes that technology itself, with its specificities, brings about (see Ch. 4, § 4.3 below).

Technology neutrality – entailing the possibility of one specific regulation, to be equally applicable to any technological situation – inevitably leads to ineffectiveness and inefficiency in governing those very aspects that require specific attention by legislators. Ultimately, selection will inevitably operate *ex post,* with everyday application, for only those technologies for which the rules appear to be *de facto* appropriate – considering the incentives they provide – will be litigated before courts on those grounds. This is precisely what occurred with the Product Liability Directive (henceforth PLD; see Ch. 3, § 3.3).

Regulation, instead, should be conceived as an evolving tool or as a living body that is to be modified together with technological advancement through a constant and attentive monitoring of emerging solutions and their specific impact on individual and social rights, as well as on the socio-economic structure of our society.

Finally, AI will penetrate the most diverse fields of human activity, such as the medical, financial and consumer products and services fields, to name a few examples. Ultimately, regulating AI will entail regulating the use of some AI-based solutions in those sectors. Therefore, given that those so diverse fields are today separately treated and governed by ad-hoc legislation, the same should happen when more technologically advanced tools start replacing more traditional ones to achieve similar if not identical outcomes. Said otherwise, the «AI effect», described above, will also make any eventual general regulation of AI disappear in the medium-run.

# 2. AI-BASED APPLICATIONS AS PRODUCTS, AND ELECTRONIC PERSONHOOD

### AI as product and the absence of a responsibility gap

13. All AI-applications and machines are products. There are no technical, philosophical, or legal considerations that justify considering machines as moral or legal agents due to their intrinsic characteristics – autonomy, the ability to learn and modify itself over time, the ability to pursue a given end independent of human supervision or control– [§ 2.1.22.1.1].
14. There is no responsibility gap. It is always possible to identify a human being who might be deemed responsible for damages arising from the production, operation and use of a machine or AI-system, based on different legal criteria. [§ 2.1.1].

### Attributing legal personhood to AI on functional grounds

15. Legal personhood is a legal fiction, primarily used with corporations to (i) achieve coordination between different parties (replacing contracts), (ii) separate assets, and limit liability, (iii) differentiate tax treatment from that reserved to natural persons [§ 2.2].
16. Similarly, a given class of AI-based applications may be attributed legal personhood on functional grounds, when that is deemed preferable to alternative legal solutions, for reasons that need to be justified on a case-by-case basis [§ 2.3].
17. Functional ground (i): identifying a *prima facie* single responsible party towards the victim, when it is impossible, or too costly for a claimant to identify the agent(s) primarily in control of the risk posed by the AI-based product or service, or benefiting from it. This might be relevant when the AI-based product or service is provided through the involvement of multiple parties that create, train, manage and offer essential services (such as in the case of an expert system used for consultancy), that are hard to disentangle, isolating responsibility on one specific agent [§ 2.3].
18. Functional ground (ii): allowing assets segregation, as a more claimant-friendly way of limiting liability, than setting a maximum amount of damages through a specific normative provision [§ 2.3].
19. Functional ground (iii): imposing registration and disclosure duties, easing the identification of those parties who bear an interest in the AI-based product or service (e.g.: AI-based software used on stock markets) [§ 2.3].

The European Parliament in the 2017 European Parliament Resolution on Civil Law Rules on Robotics (henceforth "CLRR") stated that:

> «creating a specific legal status for robots in the long run, so that at least the most sophisticated autonomous robots could be established as having the status of electronic persons responsible for making good any damage they may cause, and possibly applying electronic personality to cases where robots make autonomous decisions or otherwise interact with third parties independently»[47].

This statement caused a relevant debate, for it was interpreted as the acknowledgment of rights of robots, and more broadly machines.

[47] European Parliament (2017). European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)., paragraph 59.

As a consequence, an open letter[48] was redacted by a number of intellectuals harshly criticizing said statement as being inappropriate – both from a legal and ethical standpoint – given that there would not be any existing model on which such personality could be based.

According to the subscribers of the letter, «a legal status for a robot can't derive from the natural person model, since the robot would then hold human rights», nor from « the legal entity model, since it implies the existence of human persons behind the legal person to represent and direct it», which is not the case for robots. Lastly, – it is argued – even the Anglo-Saxon model of trust cannot represent a viable alternative since it requires specialized competences and it would still imply the existence of a human being as a last resort.

This opposition was also shared by the European Economic and Social Committee, which in its 2017 opinion on AI opposed «the introduction of a form of legal personality for robots or AI», as it believed that such solution «would hollow out the preventive remedial effect of liability law», since «a risk of moral hazard arises in both the development and use of AI and it creates opportunities for abuse»[49], without, however, further clarifying the rationale for such conclusions.

A similar position, yet based on a more articulate and also functional reasoning, was reached in 2019 by the Expert Group on Liability and New Technologies appointed by the European Commission (henceforth the "EG"), who also denied the necessity to adopt the notion of electronic personhood in the Report on Liability for Artificial Intelligence, by stating that:

> «there is currently no need to give a legal personality to emerging digital technologies. Harm caused by even fully autonomous technologies is generally reducible to risks attributable to natural persons or existing categories of legal persons, and where this is not the case, new laws directed at individuals are a better response than creating a new category of legal person. Any sort of legal personality for emerging digital technologies may raise a number of ethical issues. More importantly, it would only make sense to go down that road if it helps legal systems to tackle the challenges of emerging digital technologies. Any additional personality should go hand-in-hand with funds assigned to such electronic persons, so that claims can be effectively brought against them. This would amount to putting a cap on liability and – as experience with corporations has shown – subsequent attempts to circumvent such restrictions by pursuing claims against natural or legal persons to whom electronic persons can be attributed, effectively 'piercing the electronic veil'. In addition, in order to give a real dimension to liability, electronic agents would have to be able to acquire assets on their own. This would require the resolution of several legislative problems related to their legal capacity and how they act when performing legal transactions»[50].

Such considerations are largely, yet not completely, agreeable upon, in particular due to the excessive degree of generalization.

Radically excluding the utility of such a concept for all sorts of technologies that are both already existing and under development appears too bold and insufficiently justified a statement. While it is certainly true that in a vast majority of cases – in particular for those technologies already diffused –

[48] The open letter may be found at http://www.robotics-openletter.eu/ (last accessed June 29th 2020).

[49] European Economic and Social Committee (2017). Opinion of the European Economic and Social Committee on 'Artificial intelligence - The consequences of artificial intelligence on the (digital) single market, production, consumption, employment and society' (own-initiative opinion) , paragraph 1.12.

[50] Techno (2019). Report on Liability for Artificial Intelligence and other emerging digital technologies., 38 https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608. Bryson, J. J. and P. P. Kime (2011). Just an artifact : why machines are perceived as moral agents. Proceedings of the Twenty-Second International Joint Conference on Artificial Intelligence: Barcelona, Catalonia, Spain, 16–22 July 2011. T. Walsh. Menlo Park, CA, USA AAAI Press. II: 1641-1646.

such a notion would be superfluous, and identifying a human responsible for the harmful consequences would prove more efficient, the same cannot be vaguely generalized in all possible cases.

It would instead prove more useful, from a policy-making perspective, to identify and discuss those criteria that, if displayed by some applications could suggest such a notion to be useful (see §§ 2.2 and 2.3 below).

However, before proceeding any further, a more analytical discussion on the notion of «electronic personhood» is necessary, distinguishing among its two possible alternative interpretations, namely ontological (see § 2.1 below) and functional (see § 2.2 below) respectively.

## 2.1. The two possible interpretations of the notion of «electronic personhood»

Some of the criticism attracted by the European Parliament's statement are not analytically sound and, thence, may not be shared. At times, such critiques respond to the fear that granting a legal personality to machines would mean equating them to human beings and, in particular, granting them the same legal rights we enjoy. However, despite legitimate, these fears may easily be avoided by clarifying that machines are indeed products[51]; thus, they do not, *per se*, exclude the feasibility of an artificial legal personhood. In other occasions, such as in the EG' report, analytical and functional considerations are generalized as to apply indistinctively to a broad spectrum of technologies, such as those falling under the notion of AI, as previously defined. Yet, some applications, due to their specific features, the market where they operate, and the type of use they are destined to, may indeed raise different social and legal issues, so that it is the very same functional perspective that may allow the legislator to opt for granting them a specific form of legal personality.

However, the statement of the Parliament may give rise to different interpretations. In particular, it uses a term – «electronic personhood» – that does not yet exist, as a legal concept, in any MS's legal system, and thence appears to be different from those already existing, and widely applied, such as that of legal personhood.

On the one hand, this would lead us to imagine that electronic personhood is something different from legal personhood, possibly implying the recognition of a specific set of «robotics' rights and duties». Indeed, when a rational legislator uses a different term, it normally does so precisely to distinguish the new category – or notion –, from the existing ones.

On the other hand, what we just said is not always true in practice, and some uncertainty resides in the interpretation of a notion, when it appears to be replacing an already existing one[52]. Most importantly, the CLRR do not envisage any specific set of rights and duties which robots and AI application should be entitled to. Thence, this would lead us to believe that electronic personhood is just another way for referring to some kind of legal personhood.

[51] Bertolini, A. (2013). "Robots as Products: The Case for a Realistic Analysis of Robotic Applications and Liability Rules." Law Innovation and Technology 5(2): 214.

[52] An example is provided by the notion of «responsabilità genitoriale» introduced under Italian law to replace that of «potestà» that was deemed too tightly associated with an idea of power and dominion of the parents over the children that would not reflect the current social understanding of parents-children relationship, even in a legal perspective. However, the notion of «potestà» genitoriale had already evolved in scholarly interpretation and case law, not only in light of family law reforms, and social advancements occurred since the entering into force of the Italian civil code. Thence, the changing of the term primarily served political reasons rather than legal ones, giving rise to a complex debate, aimed at determining what had truly changed under Italian law, due to the introduction of the new term. See De Cristofaro, G. (2014). "Dalla potestà alla responsabilità genitoriale: profili problematici di una innovazione discutibile." Nuove Leggi Civili Commentate., 782. Cianci, A. (2015). La nozione di responsabilità genitoriale. La riforma della filiazione. C. M. Bianca. Padova.,779. Sesta, M. (2015). Filiazione (diritto civile). Enciclopedia del diritto. Milano. VIII., 445.

Discussing which of these solutions the European Parliament was actually endorsing with its statement would be aimless, and, most importantly, irrelevant for the purpose of this study. The proposal of the Parliament is not binding regulation, and thence the reconstructions of legislator's intention is not compelling.

Rather than focussing on reconstructing the intention of the European Parliament, we should thus discuss the overall feasibility and opportunity of the two interpretations, to understand which one, if any, should be supported in future policies.

In particular, pursuant to the first interpretation, introducing electronic personhood would support an ontological claim, that considers the machines as a different – maybe intermediate[53]– category in between things and human beings (see § 2.1.1). According to this claim machines, if sufficiently advanced (i.e. intelligent, capable of learning and of self-determining), might be deemed legal subjects – and agents – possessing rights, duties and obligations, eventually capable of being held responsible.

Under an alternative interpretation, electronic personhood would not express a new type of subjectivity, but rather grant an artificial form of legal personality due to functional considerations. In this sense machines do not possess rights and could not be deemed persons, nor intermediate beings, but might require resorting to a fictional notion comparable – and maybe identical – to that of legal persons, for purely practical purposes of better handling liability claims or other legal claims that might involve the use and/or exploitation of advanced technologies (§ 2.1.2).

### 2.1.1. Electronic personhood as the acknowledgment of individual rights of the artificial agent: radical inadmissibility

There are no technological, philosophical, nor legal reasons to deem machines as neither equal to human beings, nor belonging to an intermediate category to be distinguished between the two.

In particular, machines are things, products and artefacts of human intellect[54], and there are no ontological grounds to justify their equation to humans, so long as they do not display such a form of strong autonomy that amounts to freedom of self-determination in the outcomes the system pursues and in the ways it chooses to accomplish them[55]. Currently there is no machine that would be able to display such a level of autonomy, and there is no reason to desire the development of such a system that being more intelligent and capable than any human life form, and being also independent, could pursue its own intended ends[56].

Technological development does not justify acknowledging such a level of autonomy on the side of any AI application existing or being developed. If technically possible, such devices should be banned, for they would be intrinsically dangerous, materializing some of those dystopic accounts that might be derived from science fiction[57].

---

[53] Calo, R. (2011). "Open Robotics." Maryland Law Rev. 70.

[54] Bertolini, A. (2013). "Robots as Products: The Case for a Realistic Analysis of Robotic Applications and Liability Rules." Law Innovation and Technology 5(2): 214.

[55] Gutman, M., B. Rathgeber and T. Syed (2012). Action and Autonomy: A hidden Dilemma in Artificial Autonomous Systems. Robo- and Informationethics. Some Fundamentals. M. Decker and M. Gutman, Lit Verlag: 231-256.

[56] Koops, B.-J., Hildebrandt-Mireille and D.-O. Jaquet-Chiffelle (2010). "Bridging the Accountability Gap: Rights for New Entities in the Information Society?" Minnesota Journal of Law, Science & Technology 11(2): 497.

[57] Such as the statement of Stephen Hawking that «the development of full artificial intelligence could spell the end of the human race» available at https://www.bbc.com/news/technology-30290540 (last accessed June 29th 2020)

Absent that level of sophistication, a human being can always be identified who might be deemed responsible for the machine's output, no matter how independent or capable of self-modification the system is[58].

The so-called «responsibility gap»[59], arising from machines displaying emergent behaviour[60] is at most a misperception. Indeed, a human being is always responsible for:

Having conceived – designed and/or programmed – the system that way, attributing certain capacities and/or characteristics. The same machine could, in fact, be designed taking possible risks associated with its future performance into account, thence suggesting the adoption of alternative approaches into consideration. To exemplify, instead of opting for unsupervised learning or even allowing the machine to modify itself through its very operation, after the system is deployed or distributed, supervised and/or centralized learning approaches, that would allow the monitoring, testing, and eventually re-certification of the entire system, ought to be deemed preferable, and thence should be chosen by designers, if that allowed the minimization of risks or their control. In a civil liability perspective, should a harmful outcome arise from the functioning of the system whose conception did not abide this principle, it would not be neither unfair nor incoherent with the existing liability framework to hold the producer or designer responsible.

(i) Having used the system in the given circumstances, and/or setting, eventually adopting adequate measures to prevent or limit risks for third parties. The very choice to use a given technologically advanced device might justify the responsibility of the user, should he fail to exert adequate control over it, and avoid damages to third parties. This again, reflects a simple principle present in all legal systems, whereby if one derives an advantage from using something he should also bear the consequences of his choice.

(ii) Having modified, and/or altered the system, eventually teaching it to perform actions that result being dangerous and harmful for third parties, the rationale being identical to the one under sub (ii) above. Such a scenario could also justify the responsibility of the designer for the reasons summarized under sub (i) above, should the decision to make the system easily modifiable, and/or improvable by the user be deemed excessively risky or altogether unreasonable.

Choosing which subject to hold responsible, and thence – in a civil law perspective – burden with compensating damages, is a matter of a complex analysis that ought to be made dependent upon functional considerations of (a) efficiency and (b) effectiveness, aimed at shaping the best possible incentives for all players involved, ultimately allowing the development of desirable technologies, but also ensuring victim compensation under all circumstances [61] (see Ch. 5, § 5.2).

However, it is never sensible to deem the machine morally responsible, for it did not choose to act in a given way, and has no intentionality that might be shaped through *ex ante* incentives, such as those that legal sanctions might provide. Said otherwise, the machine can neither be blamed nor coerced for it does not fear the sanction, given that it does not perceive nor value its existence and seek to preserve it for its own sake. In such a perspective, even the punishment that might be directly inflicted onto the machine, including its disconnection, disabilitation and destruction[62] would instead solely burden

[58] Bertolini, A. (2013). "Robots as Products: The Case for a Realistic Analysis of Robotic Applications and Liability Rules." Law Innovation and Technology 5(2): 214.

[59] Matthias, A. (2010). Automaten als Träger von Rechten, Logos Verlag.

[60] That is behaviour that might not be clearly anticipated by the person who conceived the system in light of the system's complexity and ability to self-modify.

[61] Bertolini, A. (2016). "Insurance and Risk Management for Robotic Devices: Identifying the Problems." Global Jurist(2): 1-24.

[62] Floridi, L. and J. W. Sanders (2004). "On the Morality of Artificial Agents." Minds and Machine 14: 349–379.

those parties who own it, or possess rights over it. Ultimately, there are no admissible ontological grounds to deem the machine an agent, thence a subject responsible for its conduct.

Therefore, if the notion of electronic personhood were to be understood as a way to acknowledge the possibility for the machine to be granted rights, or be burdened with duties and obligations, in light of its intrinsic characteristics – intelligence, ability to learn and modify itself, autonomy, unforeseeability of its outcome – that cause it to be different from other objects, such a proposal ought to be disregarded and denied.

### 2.1.2. Electronic personhood as the equivalent of legal personhood

The second alternative is that of considering electronic personality as an (i) identical or (ii) only similar notion to that of legal personhood, and thus respond to a functional perspective. In this case, the artificial legal concept is adopted for purposes that are unrelated to the nature or ontology of the object observed – namely the machine – and are instead dependent upon technical legal considerations that might resort to a functional – including law-and-economics-based – assessment of the incentives provided by extant legislation, and the specific problems connected to the use of those applications.

In such a perspective, radically denying legitimacy to the notion of «electronic personhood» appears apodictic. Indeed, since it is not based on the intrinsic characteristics of the object regulated, thence differentiating from other artefacts, but solely on a functional assessment, the conclusion needs to be based on the evaluation of the pros and cons of attributing such personhood to machines. However, and differently from what the Expert Group on Liability and New Technologies (EG) did in its report, this evaluation may not be done for once and for all with regard to all technologies, or particularly broad and non-categorized notions of technologies, such as that of AI (Ch. 1, § 1.3), which has very little normative value. On the contrary, we need to assess the opportunity of granting legal personality with respect to precisely defined criteria, to be observed in the specific case or, better, with respect to single classes of applications[63], and the peculiarities they display in terms of (i) incentives, (ii) distribution of risks, (iii) possible cooperation of multiple human agents, as well as (iv) market structures. All such elements might influence a sound analysis leading to the identification of the preferable regulatory solution[64]. It is clear, and it will be further discussed below (see Ch. 3, § 3.5 and Ch. 4, § 4.3) that law is never technology neutral and it is not sensible to overlook technological differences and the need for specific approaches in favour of general and all-encompassing solutions.

To this end, we will first discuss the reasons that typically justify the attribution of legal personhood to artificial entities, in particular in its application to corporate law (see § 2.2), and then we will discuss with an analogic reasoning, when those conclusions might apply to advanced technologies as well, and we will attempt to draw some hypothesis, identifying criteria upon which a functional analysis can be based (see § 2.3).

## 2.2. The functional dimension of the notion of legal person in modern legal systems: considerations derived from corporate law

In all legal systems, corporations are deemed legal subjects, thence agents, capable of operating within the system, by acquiring and transferring rights. For this very reason, they might also be deemed responsible on civil law grounds – being bound to compensate damages caused during and through their operation – as well as on administrative – in case of violation for instance of environmental,

[63] Leenes, R., E. Palmerini, B.-J. Koops, A. Bertolini, P. Salvini and F. Lucivero (2017). "Regulatory Challenges of Robotics: Some Guidelines for Addressing Legal and Ethical Issues." Law Innovation and Technology: 1-44.

[64] Bertolini, A. (2016). "Insurance and Risk Management for Robotic Devices: Identifying the Problems." Global Jurist(2): 1-24.

competition, and market regulation – and, in some cases at least, criminal law grounds[65]. At the same time, natural persons might possess rights upon the corporation – being shareholders – or engage in legal interactions with it as creditors, or, more simply, as contractual counterparts.

While it is clear that the acknowledgment of the legal status of person in the case of corporations – and associations alike – does not entail the recognition of any moral or ethical status of the entity, nor the possession of human-like traits, it might be useful to point out what technical legal purposes such an attribution serves. That is indeed the indefectible presupposition for any form of analogical reasoning we could think of performing in the case of advanced technologies. Coordination and simplification, the separation of assets and limited liability, as well as the possibility to differentiate taxation will be, thence, discussed.

A corporation serves as a nexus of contracts where the entity, acting as a single party, coordinates all activities and performs all the contracts entered into with consumers, producers, employees, and other third parties[66], being liable for the obligations so assumed, as well as for the possible damages caused.

Such a coordinated role is beneficial for both the company and its creditors alike.

Indeed, both the internal organization of the corporation and its external relations could be replicated via contract law[67]. An employment contract could be in fact undersigned by all the shareholders on the one hand and the single employee on the other hand. Eventually the shareholders could stipulate a legal mandate for a representative to hire all needed personnel and conduct relevant activities. This natural person could then enter into a more complex contractual relationship with other parties who would alternatively serve as consultants or collaborators, or contribute by providing raw materials, and finally purchasing finished products and services.

In this scenario, the introduction of legal personhood is justified in terms of greater efficiency. The organization or coordination function of production was initially vested upon the price mechanism as it was considered that price movements direct production, which is in turn co-ordinated through a series of exchange transactions on the market, as «supply is adjusted to demand, and production to consumption by a process that is automatic, elastic and responsive»[68].

The firm appeared as an alternative and more efficient method of co-ordinating production since it reduces transaction costs, enabling the management of given resources by an enterprise[69]. This increased organizational efficiency also comes to the advantage of creditors, who, absent such an intermediate entity, would have to pursue individual shareholders.

Nevertheless, such a benefit would be diminished without corporate law's construct of a separate patrimony, since the latter allows for the company to own assets that are distinct from the property of its shareholders and investors, and it also allows for such property to be pledged to its creditors[70]. In this case, a company's creditors have priority in recovering their losses from company's assets, prior to

[65] This is the case with Article 5 of the Belgium Criminal Code which provides for criminal liability of legal persons for offences that are either intrinsically linked to the realisation of its purpose or the promotion of its interests, or that, as it would appear from the precise circumstances, have been committed for its account. Also, Article 121-2 of the French Criminal Code provides that legal persons are criminally liable for the offences committed for their account by their organs or representatives.

[66] Kraakman, R., P. Devies, H. Hansmann, G. Hertig, K. Hopt, H. Kanda and E. Rock (2006). The Anatomy of Corporate Law: A Comparative and Functional Approach.

[67] Ibid., 2.

[68] Coase, R. H. (1937). "The Nature of the Firm." Economica(November)., 388.

[69] Ibid., 391 ff.

[70] Kraakman, R., P. Devies, H. Hansmann, G. Hertig, K. Hopt, H. Kanda and E. Rock (2006). The Anatomy of Corporate Law: A Comparative and Functional Approach.

the claims that the personal creditors of a shareholder may have – which might be defined as «affirmative asset partitioning»[71].

Another important element of protection of a company's creditors is that of «liquidation protection» which provides that the shareholders «cannot withdraw their share of firm assets at will, thus forcing partial or complete liquidation of the firm, nor can the personal creditors of an individual owner foreclose on the owner's share or firms assets»[72]. This characteristic protects the company's creditors against voluntary insolvability and secures the existence of assets for the purpose of recovering debts or damages.

Finally, and most importantly, the company's legal personality works to the benefit of its owners and shareholders by limiting the liability of the company in the detriment of its creditors by not allowing them to foreclose the shareholder's assets[73]. This provides incentives for economic growth and the creation of corporations – essential for societal and economic cooperation – as investors would be hesitant in accepting the *alea* where all their assets are at stake.

Clearly, such limitation of potential liabilities to the assets invested in the corporation could lead to abuses, allowing owners to radically escape liability. In such cases, however, the corporate veil may be pierced[74].

Against this background, concluding, as the EG does with respect to AI applications, that granting legal personality to technological application would be rejected, because it would lead amount to a liability cap and, thus, result in «attempts to circumvent such restrictions by pursuing claims against natural or legal persons to whom electronic persons can be attributed, effectively 'piercing the electronic veil'»[75], is erroneous.

First of all, all legal rules allow for both open violations and abusive applications, where the legitimate legal tool is distorted so as to achieve outcomes that were unintended by the policy-makers who adopted it. Nevertheless, such possible outcomes are commonly anticipated, and sanctions are *ex ante* put into place to contrast them, and courts' *ex post* intervention – also through elastic notions such as good-faith, diligence and reasonableness – allows for further sorting and reaction against less obvious violations of the norms' rationale and scope. Indeed, if the utility of a given legal concept were to be judged based upon possible violations alone, most norms and the corresponding legal concepts, ought to be criticized and rejected. Instead, legal reasoning, scholarship, and case-law provide the necessary tools to tackle those unavoidable outcomes.

Furthermore, alternative mechanisms to veil piercing may be created and regulated. For example, in the case of very high risk activities undertaken by a large corporation, where veil piercing may be difficult, the law may provide for the requirement of posting a bond «equal to the highest reasonable

[71] Ibid., 424

[72] Ibid.7. In a similar vein see Posner, R. (2007). Economic Analysis of Law, Wolters Kluwer., 424 where it is stated that «the corporate form is the normal solution that the law and business practice have evolved to solve the financing and accountability problems of partnerships. The corporation's perpetual existence obviates the need for special agreements limiting withdrawal and dissolution».

[73] Posner, R. (2007). Economic Analysis of Law, Wolters Kluwer., 424.

[74] As stated in Walkovsky v Carlton «the courts will disregard the corporate form, or, to use accepted terminology, "pierce the corporate veil", whenever necessary "to prevent fraud or to achieve equity"» and «whenever anyone uses control of the corporation to further his own rather than the corporation's business, he will be liable for the corporation's acts "upon the principle of respondeat superior applicable even where the agent is a natural person"».

[75] Expert Group on Liability and New Technologies – New Technologies Formation (2019). Report on Liability for Artificial Intelligence and other emerging digital technologies., 38.

estimate of the probable extent of its tort liability»[76]. Duties to insure[77], and compensation funds[78] – admitted as possible options by the EG – might serve equal purposes[79].

Moreover, the limitation effect would neither be foreign to the extant legal system and to already applicable regulation, nor per se inadmissible.

Liability capping is indeed essential in fields such as aircraft liability[80], liability for nuclear installations[81], to name a few, and is also contemplated as a viable option in the enactment of the Product Liability Directive (henceforth "PLD") (see art. 16)[82]. Such a cap is also envisioned in the case of damages arising from the use of AI-systems[83] .

In some cases, liability capping could be essential to make a legal risk manageable also through insurance or insurance-like mechanism, allowing for the diffusion of desirable technologies and ensuring at once adequate victim compensation[84].

As anticipated, in some cases, corporations are also directly attributed criminal liability[85]. Said solutions appear to violate the principle whereby *societas delinquere non potest*. Indeed, corporations per se do not possess *mens rea*, thence their sanctioning still does not entail the acknowledgment of an ontological status as autonomous individuals. Instead, it is intended as a purely instrumental concept to punish relevant violations, in particular – yet non-exclusively [86]– in cases of money laundering, tax evasion and bribery[87]. Thus, the increasing role and involvement of corporations in many areas of the economy and society, coupled with opaque and seemingly uncontrollable nature of their

---

[76] Posner, R. (2007). Economic Analysis of Law, Wolters Kluwer., 438

[77] Expert Group on Liability and New Technologies - New Technology Formation (2019). Report on Liability for Artificial Intelligence and other emerging digital technologies., 61-62. Draft Report with recommendations to the Commission on a Civil liability regime for artificial intelligence (2020/2014(INL)), European Parliament., art. 4 (4), 18-19.

[78] Expert Group on Liability and New Technologies - New Technology Formation (2019). Report on Liability for Artificial Intelligence and other emerging digital technologies., 62 -63. Draft Report with recommendations to the Commission on a Civil liability regime for artificial intelligence (2020/2014(INL)), European Parliament., art. 4 (4), 18-19.

[79] Anderson, J. M., P. Heaton and S. J. Carroll (2010). The U.S. Experience with No-Fault Automobile Insurance. A retrospective. Santa Monica (CA), Rand. Draft Report with recommendations to the Commission on a Civil liability regime for artificial intelligence (2020/2014(INL)), European Parliament., art. 4 (4), 18-19.

[80] Article 11 of the 1952 Rome Convention on Damage Caused by Foreign Aircraft To Third Parties on the Surface provides for limited liability for the operator of an aircraft for the damages caused to «any person who suffers damage on the surface shall, upon proof only that the damage was caused by an aircraft in flight or by any person or thing falling therefrom».

[81] Article 7 of the 1960 Paris Convention on Third Party Liability in the Field of Nuclear Energy provides for a capped liability of operators of nuclear installations.

[82] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, OJ L 210, 7.8.1985, 29–33.

[83] Article 5 of the proposed Regulation in the DR with recommendations to the Commission on a Civil liability regime for artificial intelligence provides a cap of «up to a maximum total amount of EUR ten million in the event of death or of harm caused to the health or physical integrity of one or several persons as the result of the same operation of the same high-risk AI-system» and a cap of «up to a maximum total amount of EUR two million in the event of damage caused to property».

[84] Bertolini, A. (2015). "Robotic prostheses as products enhancing the rights of people with disabilities. Reconsidering the structure of liability rules." International Review of Law, Computers & Technology 29(2-3): 116-136.

[85] Article 5 of the Belgium Criminal Code provides for criminal liability of legal persons for offences that are either intrinsically linked to the realisation of its purpose or the promotion of its interests, or that, as it would appear from the precise circumstances, have been committed for its account. Also, Article 121-2 of the French Criminal Code provides that legal persons are criminally liable for the offences committed for their account by their organs or representatives.

[86] In Italy, Article 5 of the Legislative Decree no. 231 of 8 June 2001 provides for an administrative liability of corporations for criminal offences that were committed in its interest or to its advantages by its directors, executives and other persons acting on behalf of the legal person. Further, in Germany, under the Ordnungswidrigkeitengesetz (Act on Regulatory Offences) a legal person is liable for the actions of its members including a failure to exercise control over subordinates.

[87] For example, Directive (EU) 2017/1371 on the fight against fraud to the Union's financial interests by means of criminal law expressly provides that legal persons shall be liable under this directive. Liability of legal persons in this case is essential for the protection of the EU financial interests which allow for an effective administration of the EU and for social cohesion and economic development in the EU. Further, under Article 5 of the Council Framework Decision 2003/568/JHA of 22 July 2003 on combating corruption in the private sector, Official Journal L 192, 31/07/2003 P. 0054 – 0056, Member States are required to take the necessary measures to ensure that legal persons can be held liable for bribery offences committed for their benefit by any person, acting either individually or as part of an organ of the legal person, who has a leading position within the legal person.

management[88], created the need for elaborating a separate criminal liability framework for said entities.

Creating a separate criminal liability and sanctioning framework is in terms of effectiveness preferable, as it has a stronger preventive effect by addressing the real decision- maker(s)[89], given that the decentralization and often complex management structure and multiple layers of decision could cause the identification of persons responsible for committing the offence to become extremely complex[90]. Thus, «penalizing individual members has become difficult, sometimes even impossible, because of improvability, but also because of the division of responsibility between the members»[91]. Moreover, a sanction on an individual would not have an equivalent deterrence effect so as to prevent the enterprise from committing further offences[92], while measures depriving of profits eliminate any financial incentive for the entity, still preserving the possibility to criminally pursue the individual wrongdoer.

Furthermore, corporations provide for distinct entities also for the purposes of taxation allowing a diverse treatment than that reserved to individuals. Indeed, many different reasons may justify the imposition of a separate tax on corporations, and a comprehensive account would fall outside the purpose of this study. Among those, however, tax incentives shall be considered, such as investment allowances targeted at research and development activities, which lower the costs of innovation.

## 2.3. A possible functional approach to the personhood of AI applications: the need for a Class-of-Applications-by-Class-of-Application (CbC) approach

Against this background, the position of the European Parliament – suggesting that advanced robots may be considered «electronic persons responsible for making good any damage they may cause», and that electronic personality may be applied «to cases where robots make autonomous decisions or otherwise interact with third parties independently» – could be criticized as being excessive and redundant, even in such a functional perspective.

Indeed, as the EG claims, «there is currently no need to give a legal personality to emerging digital technologies» as «harm caused by even fully autonomous technologies is generally reducible to risks attributable to natural persons or existing categories of legal persons»[93]. Said otherwise, producers, suppliers of services, deployers, and in some cases even users, already operate in a corporate form. Therefore, adding another fictive legal entity would serve no other legal purpose. Eventually, a corporation might own and operate the artificial system directly.

However, once again, the EG's criticism to a possible electronic personhood is made on general and abstract level and, thus, may not be fully shared. As recalled in § 2.1.2 above, evaluating such a policy-solution under a functional perspective requires a detailed case-by-case analysis, to see whether, considering the specific characteristic of the case at hand, another intermediate entity might be useful, e.g. because it may achieve better coordination among multiple players and stakeholders.

[88] Beck, S. (2014). Corporate Criminal Liability. The Oxford Handbook of Criminal Law, 3.

[89] Ibid., 5.

[90] Recommendation No. R (88) 18 adopted by the Committee of Ministers of the Council of Europe on 20 October 1988 and explanatory memorandum, Liability of enterprises for offences., Council of Europe., 10.

[91] Beck, S. (2014). Corporate Criminal Liability. The Oxford Handbook of Criminal Law, 3.

[92] Recommendation No. R (88) 18 adopted by the Committee of Ministers of the Council of Europe on 20 October 1988 and explanatory memorandum, Liability of enterprises for offences., Council of Europe., 10.

[93] Expert Group on Liability and New Technologies - New Technology Formation (2019). Report on Liability for Artificial Intelligence and other emerging digital technologies., 38.

Moreover, claiming, as the EG does, that the electronic personhood would simply create an additional layer to the already existing legal personhood of corporation is, strictly speaking, incorrect: a different notion of electronic personhood could allow a diversification of the characteristics of said entities, from those that instead apply to corporations, as it is already today the case with other form of organizations, such as non-profit associations and foundations.

Electronic persons could thence be seen as an alternative fictive legal entity such as those mentioned above, with a partially different regulation to account for the specificities and corresponding needs that are identified and raised by some classes of technological applications.

In such a perspective, US scholars[94] have exemplified the case of limited liability companies (LLCs), an organizational form characterized by greater degrees of freedom of its members in determining the internal structure and form of governance, still maintaining the benefits associated to limited liability and the tax regime applicable to corporations. It is argued that such LLCs could be used to grant autonomous systems an equivalent functional legal status similar to those of corporations [95] as in some cases state laws may allow for the perpetual existence of member less LLCs[96]. LLC would thence be created by a member which would then in turn leave the LLC and allow the algorithm to execute the articles of organization [97], in a similar way as the representatives of corporation do under existing legal frameworks[98].

To summarize, it may be concluded that there may be cases, now or in the future, where it might be sensible to attribute the machine some form of legal personhood. That might be achieved both (i) by extending to machines the application of the notion of legal personhood as today defined for corporations, or (ii) by creating a different notion of legal personhood such as that of electronic personhood with different regulation[99].

[94] (Bayern, 2015, 95)

[95] Bayern, S. J. (2015). "The Implications of Modern Business-Entity Law for the Regulation of Autonomous Systems." 19 Stanford Technology Law Review 93., 104, available at SSRN: https://ssrn.com/abstract=2758222.

[96] Ibid., 96.

[97] Ibid., 99.

[98] The author provides the following examples: (i) «An agreement can, by specifying obligations and conditions, effectively delegate legal rights and decision-making powers to such an algorithm even though that algorithm is not a legal person. An agreement might say, for example, "Your obligation to perform is discharged if the algorithm indicates X," where X could be (for an unsophisticated algorithm) a formal output on a computer terminal or (for an artificially intelligent algorithm) something that approaches a description of human understanding and action (like "that it is satisfied with the arrangement and physically signs a release form") » and (ii) «for example, suppose I develop a robot and open a bank account for the robot in my name, and suppose that using that account, the robot is able to earn some money from third parties. As a legal person, I simply can use the "robot's" funds to purchase a house for the robot's use, functioning as its practical, substantive, and economic (though not legal) agent. As with a trust, no new legal person needs to be created in order to permit one person to act to achieve impersonal goals. Consequently, legal personhood begins to look mostly like a bookkeeping mechanism—or like a way of simplifying the law's terminology and accounting—rather than like a substantive grant of rights». See ibid., 99 and 107.

[99] The creation of such a new form of legal personhood is not unusual, when there is an identified need in this respect. An example of a hybrid legal person is that of the European Cooperative Society (SCE) regulated under Council Regulation (EC) No 1435/2003 of 22 July 2003 on the Statute for a European Cooperative Society (SCE) OJ L 207, 18.8.2003, 1–24. The SCE's legal status and personality was recognized so as to ensure equal terms of competition and to contribute to EU's economic development by providing cooperatives, which are a form of organisation generally recognised in all Member States, with adequate legal instruments capable of facilitating the development of their cross-border activities. As per the Regulation, the SCEs «have a share capital and their members may be either individuals or enterprises. These members may consist wholly or partly of customers, employees or suppliers. Where a cooperative is constituted of members who are themselves cooperative enterprises, it is known as a "secondary" or "second-degree" cooperative. In some circumstances cooperatives may also have among their members a specified proportion of investor members who do not use their services, or of third parties who benefit by their activities or carry out work on their behalf». The principle object of the SCE is «the satisfaction of its members' needs and/or the development of their economic and social activities, in particular through the conclusion of agreements with them to supply goods or services or to execute work of the kind that the SCE carries out or commissions». Furthermore, SCEs may have limited or unlimited liability depending on the members' choice, as per Article 1 (2) of the Regulation «unless otherwise provided by the statutes of the SCE when that SCE is formed, no member shall be liable for more than the amount he/she has subscribed». Also, under the SCE, as per Recital 8, members cannot exercise any rights over the assets of the cooperative. Further, any surplus at the end of a financial year cannot be distributed to its members before a portion of at least 15% of such surplus is allocated to a legal reserve and members cannot have claims against such legal reserve (Article 65).

In both cases, what matters are the condition that ought to be met by advanced technological applications to justify such a solution.

Leaving aside consideration about the opportunity to adopt a different tax regime for advanced technologies – that could be more or less favourable in principle – which has already triggered a relevant debate[100], and falls outside the scope of the current analysis, the primary purposes for adopting the fictive notion of legal personhood are that of (i) pursuing increased efficiency in coordinating the different parties that might share interests – and risks – in the operation of a single AI-system, and (ii) segregating specific assets.

As per the first issue – that of coordination –, it shall be noted how one of the major concerns when discussing liability for damages arising from the use of advanced technologies is the difficulty in apportioning liability among multiple parties that cooperate in the creation and operation of the given application or service.

Product designers, software and other service providers – including data and infrastructure managers and providers – owners and users – professional or not – might cooperate in an intricate way in the deployment and utilization of a given device. Liability apportionment, also due to the overlapping of alternative liability regimes, could prove most complicated (see Ch. 5 § 5.2 below).

The need for simplification is evident, and necessary to ensure sufficient ease for victim's compensation. In such a perspective, the adoption of a one-stop-shop solution – pursuant to a Risk-Management Approach (henceforth "RMA")– could prove most effective, as it entails clearly identifying one responsible party, eventually through strict or even absolute liability rules (see Ch. 5, § 5.2 below)[101].

Such a solution might prove preferable in most cases. However, a theoretically viable alternative would be that of creating a fictional entity where all – or some – of the above referred parties are called in to participate, and thence contribute.

In this sense, the victim could direct her claim against the fictional entity – the technological application being granted fictitious legal personality – and thus interact with one single, clearly identified subject, whereas the complexity of the production and supply chain (e.g. for industrial robots, see § 5.4 below), as well as of the digital environment in which the technological application operates (e.g. for self-driving cars, see § 5.5 below), would make it difficult to actually identify what exactly caused the

[100] The proposal of the European Parliament in the CLRR on the so called «robot tax» has attracted, in principle, opposing reactions, including from the European Commission Vice-President Andrus Ansip which stated that it would not «be wise to impose additional taxes on robots. Robotics and artificial intelligence are essential to Europe's competitiveness. They also improve the daily life of people, at home and at work, helping with repetitive or dangerous tasks» - available at https://www.euractiv.com/section/5g/interview/ansip-additional-taxes-on-robots-would-be-unwise/ (last accessed June 29th 2020). Further the International Federation of Robotics also stated that «to tax production tools instead of their profits would have a negative impact on competitiveness and employment». -available at https://ifr.org/news/world-robotics-federation-ifr-why-bill-gates-robot-tax-is-wrong (last accessed June 29th 2020).

[101] One may look at other areas of the law and collaboration mechanism that involve the intertwined contribution of many parties, such as in construction law. The building of highly sophisticated assets, such as a hydropower plants, involves the contribution of many actors. Construction law has a couple of concepts that may be borrowed for the building of a machines as well such as the risk management matrix and the principle of allocating the risk to the party when the risk is within the party's control. The risk management matrix is a contractual tool created by the contributing partners whereby they allocate the risk from the beginning of the project - and it can be amended throughout the project – to the party that controls the risk. One may borrow such a concept for robots as well, where the participants would allocate the risks of liability. Further, a certification scheme may be put in place whereby a robot could be marketed only if certified and certification would be dependent upon providing such a comprehensive risk matrix. This would allow for the victim of a potential damage to identify the responsible party easily, without going through expensive litigation with all contributing participants.

Creating a comprehensive framework for liability allocation is still required and the intervention of the legislator is more favourable to the society than simply applying existing models. The two options presented above paint a more favourable picture than the one existing today when the collaborating partners in the development of a robot simply don't clearly allocate liability and it is for the victim to figure it out, or they decide to create a separate corporation with limited liability, which is often the case, as corporations create separate corporations for new lines of business and of products (e.g. the creation of a new robot) and thus, benefit from the shield against responsibility, which in turn is presented as one of the major risks against granting personhood to robots.

damage, and who – among the many subjects involved – was responsible for it, and under which ground of liability, leading to particular burdensome and expensive litigations. Pursuant to a RMA, this entity would ensure compensation and solvability by relying on a broad system of insurance. Ideally, the organizational structure of the entity may then allow to redistribute said costs among the different subjects who contributed to its creation, either directly, by cutting on the distribution of the profits to the party responsible for the faulty part, or indirectly, by leading to redistribution of the shares and the assets constituting the entity itself. A similar proposal comes from the EG, when advocating in favour of the acknowledgment of commercial and technological units[102].

Finally, the creation of a fictional entity might allow for a greater transparency about the different stakeholders in the device or service operation. Through registration and disclosure duties that are typically imposed on legal entities[103], it is possible to determine at any given moment in time who bears an economic and legal interest in it. Similar result might be desirable, for instance, in the case of AI-systems intended to operate in the stock market. Indeed, advanced computer programs are designed to analyse multiple markets and execute a large number of orders based on fluctuations occurring even in a small fraction of time. Such High-frequency trading (HFT) may be particularly profitable, since the traders with the fastest execution speeds make higher profits than slower ones. However, the conjunct operation of multiple HFT has been deemed as a possible contributor to crises and market collapses, as these programs tend to sell aggressively to eliminate their position in the face of uncertainty, ultimately exacerbating price declines[104]. Here, the creation of an electronic person with specific registration duties would help ensure the transparency of the overall operation and the responsibility of the entity – with its individual stakeholders behind it – for the possible mismanagement and distortive effect on the market[105].

With respect to the second profile – that of segregating specific assets – granting electronic personhood to a given technology might also allow the distribution of cash flows generated by its functioning. In turn, this may have a series of positive implications, either directly or indirectly connected with the issue of liability.

Firstly, and most importantly, asset partitioning would be the very element that, after the creation of the entity, and the attribution of an autonomous initial patrimony, would allow the technological application to «earn its own assets», thus granting its liquidity and solvability in case of damages claims (see Ch. 4 below § 4.6.8).

Secondly, granting electronic personality to an AI-based technology may offer a useful solution for redistributing the profits made by its activities especially in situations where, absent a clear legal intervention on the matter, the ownership and overall rights over the results of the machine's activity is disputed, as in the case of creation upon which the electronic person may be deemed to hold IP-law related entitlements, such as patent and copyright.

[102] See Expert Group on Liability and New Technologies - New Technology Formation (2019). Report on Liability for Artificial Intelligence and other emerging digital technologies., EG's key findings nn° 29-30, 55-56.; also see Ch. 4.6, § 4.6.3 below.

[103] See in this respect Chapter III under Directive (EU) 2017/1132 of the European Parliament and of the Council of 14 June 2017 relating to certain aspects of company law (Text with EEA relevance.) OJ L 169, 30.6.2017, 46–127, setting forth disclosure requirements for companies and branches opened in a Member State by certain types of company governed by the law of another State.

[104] Art. 2 (4o), Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU, OJ L 173, 12.6.2014, 349–496. (MiFID II): 'high-frequency algorithmic trading technique' means an algorithmic trading technique characterised by: (a) infrastructure intended to minimise network and other types of latencies, including at least one of the following facilities for algorithmic order entry: co-location, proximity hosting or high-speed direct electronic access; (b) system-determination of order initiation, generation, routing or execution without human intervention for individual trades or orders; and (c) high message intraday rates which constitute orders, quotes or cancellation; Puorro, A. P. (2013). "High Frequency Trading: una panoramica." Questioni di Economia e Finanza 198.

[105] Art. 5 MiFID II.

Thirdly, the creation of a fictional entity might allow for a greater transparency about the different stakeholders in the device or service operation. Through registration and disclosure duties that are typically imposed on legal entities[106], it is possible to determine at any given moment in time who bears an economic and legal interest in it.

Finally, asset partition may operate as a form of liability capping, which – contrary to the EG's claim –, may prove necessary to allow for the deployment of services that might be deemed beneficial and socially desirable, and yet potentially give rise to risks that might be hard to manage otherwise, similarly to those cases referred above (see § 2.2 above) where limitations are already in place.

To conclude, the reduction of market costs and increased economic productivity are factors to be taken into account when analysing the legal personality of machines as it would most likely have a co-ordinating role in production as corporations do. This is of particular importance in the case of expert systems where the major concern around liability, accountability and profitability presuppose the involvement of a large number of contributors, such as multiple software developers, multiple hardware developers and multiple services providers.

One might say that such a result could be achieved by the voluntary association of such contributors in a legal person. This is a valid argument, however, although such a voluntary association may prove efficient not only economically wise, but also accountability wise, the contributors may choose to keep the economic benefits and surplus resulting from such collaborative activity separate[107]. Electronic personhood may, thus, act not only as a co-ordinator of production, but also as a co-ordinator of liability forcing it upon the parties or allowing for a different legal tool to achieve it.

[106] Under Article 14 of the Directive (EU) 2017/1132 «Member States shall take the measures required to ensure compulsory disclosure by companies of at least the following documents and particulars: (a) the instrument of constitution, and the statutes if they are contained in a separate instrument; (b) any amendments to the instruments referred to in point (a), including any extension of the duration of the company; (c) after every amendment of the instrument of constitution or of the statutes, the complete text of the instrument or statutes as amended to date; (d) the appointment, termination of office and particulars of the persons who either as a body constituted pursuant to law or as members of any such body: (i) are authorised to represent the company in dealings with third parties and in legal proceedings; it shall be apparent from the disclosure whether the persons authorised to represent the company may do so alone or are required to act jointly; (ii) take part in the administration, supervision or control of the company; (e) at least once a year, the amount of the capital subscribed, where the instrument of constitution or the statutes mention an authorised capital, unless any increase in the capital subscribed necessitates an amendment of the statutes; (f) the accounting documents for each financial year which are required to be published in accordance with Council Directives 86/635/EEC (26) and 91/674/EEC (27) and Directive 2013/34/EU of the European Parliament and of the Council (28); (g) any change of the registered office of the company; (h) the winding-up of the company; (i) any declaration of nullity of the company by the courts; (j) the appointment of liquidators, particulars concerning them, and their respective powers, unless such powers are expressly and exclusively derived from law or from the statutes of the company; (k) any termination of a liquidation and, in Member States where striking off the register entails legal consequences, the fact of any such striking off». As per arts. 17 and 18, these documents must be available and up to date in national registries and in electronic form.

[107] As it is the case with advanced technologies, where, for example, the producer of a micro-processor might not want to associated itself with the software developer and share profits and liabilities, as the liability of the latter would proportionally diminish the former's profits.

# 3. THE EUROPEAN REGIME AND ITS ADEQUACY

**Product safety and its relationship with product liability**

20. Product safety and product liability are complimentary. The former defines under which conditions a product may be deemed safe and released onto the market. The latter identifies who shall bear the consequences of a damage caused by a product, balancing the need of ensuring users' protection and that of allowing products to be distributed for profit [§ 3.1& § 3.2].

**The PLD and its assessment**

21. The Product Liability Directive (PLD) establishes a horizontal, technology neutral system of liability, where the producer is strictly liable for damages caused by a defect in his product [§ 3.3].
22. Studies and reports commonly argue that (i) the PLD is overall relevant, effective and efficient; (ii) certain characteristics of new technologies may make it difficult for the victim to obtain compensation [§ 3.4].
23. These assessments rest on debatable empirical and theoretical premises, as the high litigation costs and the limited chances of success lead victims to activate their rights under concurrent national or EU frameworks [§ 3.4].
24. The limited success of the PLD is to be found in a series of problematic features, which are likely to be exacerbated in case of damages caused by technologically advanced applications [§ 3.4].
25. Criticality (i): the scope of application of the directive does not clearly cover damages caused by software [§ 3.4.1].
26. Criticality (ii): the victim is required to prove the damage suffered, the defect, and the causal nexus between the two, without any duty of disclosure of relevant information on the producer [§ 3.4.4].
27. Criticality (iii) compromise the strict liability paradigm adopted by the directive (i.e. reference to the standard of "reasonableness" in the notion of defect, and negligence-based assessment enshrined in the development risk defence) [§ 3.4.2 & § 3.4.3].
28. Criticality (iv): limit recoverable damages [§ 3.4.5].

**Proposed revision of the PLD**

29. The PLD should be revised as to ensure effective compensation, addressing the inefficiencies and puzzles identified in nn. 24 ff. [§ 3.5].
30. To ensure technology-specific regulation, the PLD shall constitute a general and residual rule, covering both traditional products and new technologies, while narrow tailored regulations should be adopted at the European level, for specific classes of applications [§ 3.5, § 3.6].

## 3.1. Ensuring product safety: product safety regulation

The Product Safety regime defines under which conditions a product may be deemed safe, and thus released onto the market. It also establishes a complex system of market surveillance, imposing national authorities to check whether products meet the applicable safety requirements, and to take the necessary measures for ensuring compliance.

Indeed, the realm of technical conditions prescribed directly by EU legislation is relatively finite. With the adoption of the so called «New Approach»[108], and later with the «New Legislative Framework Approach»[109], legislative harmonization was limited to the essential safety requirements – i.e. requirements that products placed on the EU market must meet – while the actual technical specifications are laid down by standards developed by international (e.g. ISO) and European organizations (e.g. CEN-CENELEC), and national authorities (e.g. UNI, DIN).[110] Technical standards, however, are not binding rules in themselves. Legal compliance is only required with directives and other pieces of legislation, and these specifications merely identify the best practice or state of the art in a given area, or with respect to a given application, which may be implemented as a way of meeting the mandatory requirements set out by EU law.

Against this background, the EU product safety legislation comprises both product- or sector- specific legislation – such as that relating to toys, electrical appliances, cars, medical devices, personal protective equipment, pharmaceuticals, etc. etc. –, and the general rules set out in the General Product Safety Directive[111] (henceforth, "GPSD"), which applies when no special rules are set for a given product or risk at the EU level. These instruments not only establish the essential technical requirements for products to be deemed safe and commercialized, but also set out specific obligations for manufacturers in the development, marketing and commercialization of their products, and the duties they hold both against consumers, as well as national and European authorities.

In particular, the GPSD requires firms to (i) ensure that products – i.e. any item intended for sale to, or likely to be used by, consumers, be it new, used or reconditioned (art. 2 GPSD) – are safe; (ii) inform consumers of any risks associated with the products supplied; and (iii) take corrective action when those products prove to be unsafe.

Under the GPSD, product safety is reached when: «[…] under normal or reasonably foreseeable conditions of use including duration and, where applicable, putting into service, installation and maintenance requirements, does not present any risk or only the minimum risks compatible with the product's use, considered to be acceptable and consistent with a high level of protection for the safety and health of persons, taking into account the following points in particular: (i) the characteristics of the product, including its composition, packaging, instructions for assembly and, where applicable, for installation and maintenance; (ii) the effect on other products, where it is reasonably foreseeable that

[108] Council Resolution of 7 May 1985 on a new approach to technical harmonization and standards, OJ C 136, 4.6.1985, 1–9.

[109] Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93, OJ L 218, 13.8.2008, 30–47; Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC, OJ L 218, 13.8.2008, 82–128; Regulation (EC) No 764/2008 of the European Parliament and of the Council of 9 July 2008 laying down procedures relating to the application of certain national technical rules to products lawfully marketed in another Member State and repealing Decision No 3052/95/EC, OJ L 218, 13.8.2008, 21–29.

For an overview of this approach, see https://ec.europa.eu/growth/single-market/goods/new-legislative-framework_en (last accessed, June 29th 2020), and, more in detail, European Commission (2016). The 'Blue Guide' on the implementation of EU products rules 2016. For a description and an assessment of the product safety framework in the field of industrial robots, see Timan, T., R. Snijders, M. Kirova, S. Suardi, M. v. Lieshout, M. Chen, P. Costenco, E. Palmerini, A. Bertolini, A. Tejada, S. v. Montfort, M. Bolchi, S. Alberti, R. Brouwer, K. Karanilokova, F. Episcopo and S. Jansen (2019). Study on safety of non-embedded software. Service, data access, and legal issues of advanced robots, autonomous, connected, and AI-based vehicles and systems: final study report regarding CAD/CCAM and industrial robots. Brussel, European Commission., Annex 3, Task 3&4.

[110] For an overview: https://ec.europa.eu/growth/single-market/european-standards/harmonised-standards_en. More in detail: European Commission, The 'Blue Guide' on the Implementation of Eu Products Rules 2016 (2016)Timan, T., R. Snijders, M. Kirova, S. Suardi, M. v. Lieshout, M. Chen, P. Costenco, E. Palmerini, A. Bertolini, A. Tejada, S. v. Montfort, M. Bolchi, S. Alberti, R. Brouwer, K. Karanilokova, F. Episcopo and S. Jansen (2019). Study on safety of non-embedded software. Service, data access, and legal issues of advanced robots, autonomous, connected, and AI-based vehicles and systems: final study report regarding CAD/CCAM and industrial robots. Brussel, European Commission. European Commission (2020). Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee. Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, European Commission., 3 ff. and, more in detail, European Commission (2016). The 'Blue Guide' on the implementation of EU products rules 2016.

[111] Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety, OJ L 11, 15.1.2002, 4–17.

it will be used with other products; (iii) the presentation of the product, the labelling, any warnings and instructions for its use and disposal and any other indication or information regarding the product; (iv) the categories of consumers at risk when using the product, in particular children and the elderly […]»(art. 2(b) GPSD).

Pursuant to the GPSD, a product is deemed safe it if meets all statutory requirements under European or national law, and it is indeed presumed safe when they conform to voluntary national standards transposing EU harmonised standards (art. 3(2) GPSD). If no such requirements or standards exist, products safety is assessed with reference to non-harmonized European and national standards, Commission guidelines on product safety assessment, product safety codes of good practices, state of the art and technology, and reasonable consumer's expectation (art. 3(3) GPSD). To ensure product safety, producers shall provide consumers with the relevant information enabling them to assess the risks inherent in the product during its normal or foreseeable time of use, taking the appropriate precautions and adopting the adequate safeguards. In particular, producers are required to take the necessary measures to be informed about the risks that their products might cause and take appropriate action to avoid them, including warning, withdrawal and recalling (art. 5 GPSD).

In addition to a general safety requirement, many products must obtain a CE mark in order to be commercialized within the EU. CE marking indicates that the product has indeed been assessed by the manufacturer to check their compliance with the essential safety requirements set out by relevant legislation. Product certification rules thus serve a twofold aim: (i) they ensure high levels of product quality and safety, ultimately strengthening the users' confidence and protection, and (ii) create uniform procedures and market-conditions, allowing free trading of goods onto the EU market[112].

If a product belongs to those for which EU specifications exist, and affixing of the CE marking is mandatory, producers shall assess conformity with all the relevant requirements according to the appropriate procedure. Each legislation has its own specific rules on the matter. However, as a general feature, it normally lays down two alternative paths: self-assessment and self-declaration, or assessment through an independent notified body, depending on the specific features of the product in question, the category and level of risk it displays, as well as whether technical standards were used to make the product safety-compliant, and – if so – which kind of standards have been deployed[113].

Indeed, and as mentioned above, compliance with technical standards normally constitutes a way for manufacturers to meet essential safety requirements, and may lead to easier assessments for the sake of product certification. This is particularly true for a peculiar type of standards, i.e. harmonized standards (hEN) developed by a recognized European Standards Organisation – CEN, CENELEC, or ETSI – following a request from the European Commission. If a product was manufactured according to hEN standard, it will be deemed conforming with the relevant essential requirements, and, in some cases, the manufacturer may benefit from a simplified assessment procedure (e.g. the manufacturer's declaration of conformity). However, it is worth stressing again that manufactures are not obliged to apply hEN or other technical standards, as non-compliance only results in the need to demonstrate

[112] For an extensive overview of this topic, see: Timan, T., R. Snijders, M. Kirova, S. Suardi, M. v. Lieshout, M. Chen, P. Costenco, E. Palmerini, A. Bertolini, A. Tejada, S. v. Montfort, M. Bolchi, S. Alberti, R. Brouwer, K. Karanilokova, F. Episcopo and S. Jansen (2019). Study on safety of non-embedded software. Service, data access, and legal issues of advanced robots, autonomous, connected, and AI-based vehicles and systems: final study report regarding CAD/CCAM and industrial robots. Brussel, European Commission.; European Commission (2016). The 'Blue Guide' on the implementation of EU products rules 2016.

[113] Timan, T., R. Snijders, M. Kirova, S. Suardi, M. v. Lieshout, M. Chen, P. Costenco, E. Palmerini, A. Bertolini, A. Tejada, S. v. Montfort, M. Bolchi, S. Alberti, R. Brouwer, K. Karanilokova, F. Episcopo and S. Jansen (2019). Study on safety of non-embedded software. Service, data access, and legal issues of advanced robots, autonomous, connected, and AI-based vehicles and systems: final study report regarding CAD/CCAM and industrial robots. Brussel, European Commission.; European Commission (2016). The 'Blue Guide' on the implementation of EU products rules 2016.

(normally through the involvement of an independent notified body) that the technical solution adopted in alternative, indeed, satisfies the essential safety requirements[114].

## 3.2. The relationship with product liability

Product safety regulation and product liability are complementary[115].

The product safety framework ensures that products traded onto the EU market are safe, and that continuous compliance with safety-requirements is guaranteed during their entire life-cycle. Mandatory specifications and procedures guide producers in the manufacturing and commercialization phase – establishing what is allowed and what is not allowed –, and are backed up with specific sanctions in case of non-compliance (withdrawal from the market, administrative fines etc.).

On the contrary, product liability, being a specific type of civil liability, addresses the separate question of whom shall pay, how much, and under which conditions, if a product causes damages, even if the commercialization of the latter was allowed under product safety rules. Indeed, art. 17 of the General Product Safety Directive (GPSD) explicitly states that the «directive shall be without prejudice to the application of Directive 85/374/EEC».

Civil liability rules deal with the consequences of a damage caused by an activity that turned out to be harmful, regardless of whether said activity was in principle allowed or not. In doing so, they ensure an economic-efficient balance of competing interests. When no outright-prohibition is in place, and an activity is allowed despite carrying some degree of risk, liability rules make sure that damages resulting from it are adequately compensated[116].

Mass-manufacturing and commercialization of products for profit carry an inherent risk, but shall be authorized because of the overall social benefit they bring about. Risks that are not deemed acceptable will be addressed *ex ante* trough product safety rules, which prohibit some products or activity, and allow others, as long as they meet all the essential safety requirements. Furthermore, the need to encourage rather than hinder socially-valuable activities also affects the extent and conditions of recoverable damages. If the negative outcome corresponds to a level of risk that is deemed desirable for society, then the damage shall stay with the victim, or be indemnified through alternative mechanisms – e.g. no-fault based compensation schemes, mandatory insurance – not directly burdening the producer or programmer of the machine, since said activity needs to be encouraged rather than opposed (see § 3.5; and Ch. 4). If, on the contrary, the level of risk introduced is not acceptable, the harmful event caused by the product will be considered illicit and the cost of the infringement will be shifted back on the person responsible for causing it. Under EU law, this balance is primarily centred on the notion of «defect», as only damages caused by a defective product may be compensated[117]. As indicated below, for the purpose of the European rules on product liability, a

---

[114] Timan, T., R. Snijders, M. Kirova, S. Suardi, M. v. Lieshout, M. Chen, P. Costenco, E. Palmerini, A. Bertolini, A. Tejada, S. v. Montfort, M. Bolchi, S. Alberti, R. Brouwer, K. Karanilokova, F. Episcopo and S. Jansen (2019). Study on safety of non-embedded software. Service, data access, and legal issues of advanced robots, autonomous, connected, and AI-based vehicles and systems: final study report regarding CAD/CCAM and industrial robots. Brussel, European Commission. "Study on Safety of Non-Embedded Software", European Commission, 209.

[115] European Commission, (2020). Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee. Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, European Commission., 12.

[116] Bertolini, A. (2014). Robots and liability - Justifying a change in perspective. Rethinking Responsibility in Science and Technology. F. Battaglia, J. Nida-Rümelin and N. Mukerji. Pisa, Pisa University Press: 143-166. Palmerini, E. and A. Bertolini (2016). Liability and Risk Management in Robotics. Digital Revolution: Challenges for Contract Law in Practice. R. Schulze and D. Staudenmayer. Baden-Baden, Nomos: 225-259.

[117] Bertolini, A. (2014). Robots and liability - Justifying a change in perspective. Rethinking Responsibility in Science and Technology. F. Battaglia, J. Nida-Rümelin and N. Mukerji. Pisa, Pisa University Press: 143-166. Palmerini, E. and A. Bertolini (2016). Liability and Risk

product is «defective when it does not provide the safety which a person is entitled to expect, taking all circumstances into account, including: (a) the presentation of the product; (b) the use to which it could reasonably be expected that the product would be put; (c) the time when the product was put into circulation» (art. 2 PLD).

Against this background, it is important to highlight that product safety rules and product liability rules work in synergy, but operate at essentially different levels, according to different principles and conditions.

Indeed, if a product turns out to be dangerous after being released onto the market, manufacturers have a duty to take all the necessary measures to prevent the risk from materializing, i.e. withdrawing it from the market and recalling it from its users. By doing so, they may avoid the causation of any damage, and exclude the application of liability rules.

On the contrary, a product that is deemed safe for it satisfies all applicable requirements may still be defective and cause damage. Compliance with safety regulation does not shield producers from product liability. Even the fact that a given product was «certified» (or self-certified) does not *per se* exclude, for example, that one specific item in the batch turns out to be defective, or that its use may lead to defects and accidents that were not envisaged at the time of manufacturing, possibly causing the producer to be held liable pursuant to product liability rules (for a description of the so-called «manufacturing defect» and «design defect», see § 3.33.3 below).

Likewise, compliance with technical standards does not exclude manufactures from product liability claims. Conversely, non-compliance with said standards does not entail that the product is defective. As explained before, manufacturers may have resorted to other tools to demonstrate that the product fulfils the essential safety requirements (see Ch. 4, § 4.6.6 and the criticism that ca be drawn on this point to the EG report). For the purpose of a liability claim, they will have to demonstrate that the product was not defective.

## 3.3. The Product Liability Directive: an overview

The PLD[118] constitutes the main reference for product liability rules under EU law.

As anticipated above, the PLD serves two overall functions: (i) balancing the need not to hinder socially economic activities and technological progress, with that of granting a fair allocation of the risks and costs arising thereof, through rules that ensure safe products and adequate compensation, (ii) harmonizing national rules on product liability, to ensure high level of consumer protection and fair competition among businesses across MS, thus contributing to the establishment of the internal market[119].

Indeed, the recitals of the directive clarify that the PLD aims at ensuring high level of consumer protection in an «age of increasing technicality [through] of a fair apportionment of the risks inherent in modern technological production». Thus, the PLD establishes a «liability without fault on the part of the producer», which is presented as «the sole means of adequately solving the problem» of risk distribution. In particular, since the PLD «protects the physical well-being and property of the consumer […] the defectiveness of the product should be determined by reference not to its fitness for use but to the lack of the safety which the public at large is entitled to expect».

---

Management in Robotics. Digital Revolution: Challenges for Contract Law in Practice. R. Schulze and D. Staudenmayer. Baden-Baden, Nomos: 225-259. In the American Law and Economic doctrine, see Posner, Richard. 2007. Posner, R. (2007). Economic Analysis of Law, Wolters Kluwer.

[118] For an overview of the directive and its implementation among Member States, see Machnikowski, P. (2016). European Product Liability. An Analysis of the State of the Art in the Era of New Technologies. Cambridge, Intersentia.

[119] See PLD, recitals.

In addition to this, the PLD also aims at «approximat[ing] the laws of the Member States concerning the liability of the producer for damage caused by the defectiveness of his products […] because the existing divergences may distort competition and affect the movement of goods within the common market and entail a differing degree of protection of the consumer against damage caused by a defective product to his health or property».

As for its actual regime, the PLD provides exhaustive harmonization of liability rules regarding damages caused by defective products, but leaves untouched non-harmonised national legislation, so that the injured party may still rely on national provisions on damages based on contractual liability, or non-contractual liability other than product-specific ones. It establishes a technology neutral and horizontal regime, primarily centred on the notion of traditional movable, mass-produced and tangible products, used by consumers.

Pursuant to the directive, «the producer shall be liable for damage caused by a defect in his product», and liability will indeed be established upon evidence of the damage, the defect, and the causal nexus between the two (art. 1 PLD).

Producers are described as «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, trade mark or other distinguishing feature on the product presents himself as its producer» (art. 3 PLD). Those who import products from outside the EU for any kind of distribution in the course of their business are also considered producers for the purpose of the PLD. Furthermore, the supplier of the product will be subject to the same liability, unless she informs the injured person, within a reasonable time, of the identity of the producer or of the person who supplied the product to him.

Products are intended as «all movables, with the exception of primary agricultural products and game, even though incorporated into another movable or into an immovable» (art. 2 PLD). They are considered defective, when they «do not offer the safety that a person is entitled to expect, considering all circumstances», including the presentation of the product, its reasonably expected use, and the time in which it was put into circulation (art. 6 PLD). On the contrary, a product shall not be deemed defective merely because a better one was put into circulation later on (art. 2 PLD).

Legal scholarship has classified the possible defects into three categories. If a single item deviates from the intended design, and thus does not conform to the batch of the other mass-produced products, the defect affecting the product constitute a «manufacturing defect». If information and warnings concerning the potential dangers deriving from the use of the devise are not adequately communicated, we face an «information defect». Finally, if it's the very design of the product that does not guarantee the required level of safety, or is unreasonably dangerous, the product will be deemed affected by a «design defect». Despite not having explicit legal relevance, the aforementioned distinction offers a useful conceptual tool to analyse the concrete functioning of the product liability regime, as well as to assess its effectiveness, because – as we will see in §§ 3.4 and especially § 3.4.2, § 3.4.3 and § 3.4.4 below – the position of the claimant in a product liability case varies considerably depending on the type of defect involved (e.g. as far as the evidentiary burden is concerned), and so does the capacity of the producer to escape liability (e.g. the state of art defence only applies for defective design).

According to the PLD, producers, or the subject identified by art. 3 (the importer of a product within the EU, and the seller of the product, whenever the producer cannot be identified), are held liable to compensate for the damages caused from the use of the product, provided that product is defective, and there is a causal nexus between the defect and the damage which compensation is sought for (art. 4 PLD). To succeed in the claim, the victim is required to prove the three constitutive elements of its cause of action: i.e. the damage, the defect and the causal nexus. Since she does not need to prove that the producer was at fault, the producer is held objectively liable. However, she may escape liability by relying on one of the exonerating circumstances set out in art. 7, namely:

a) s/he did not put the product into circulation;

b) it is probable that the defect did not exist at the time when the product was put into circulation, or that it came into being afterwards;

c) the product was neither manufactured for sale or any form of distribution for economic purpose, nor manufactured or distributed in the course of his business;

d) the defect is due to compliance with mandatory regulations;

e) the state of scientific and technical knowledge at the time the product was put into circulation was not such as to enable the existence of the defect to be discovered; however, pursuant to art. 15, MS may derogate from this provision and extent liability also to cases falling within this circumstance.

f) in case of a manufacturer of a component, that the defect is attributable to the design of the product in which the component has been fitted or to the instruction given by the manufacturer of the products.

Furthermore, proof of contributory negligence from the injured person may lead to reduce or disallow producer's liability. On the contrary, liability may not be reduced if a third party's act or omission contributed in the causation of the damage (art. 8 PLD).

In case multiple persons are responsible for the same damage, they are held jointly and severally liable under EU law, while national provisions may apply for internal distribution of the damage, on the basis of contribution or recourse actions (art. 5 PLD).

Limits are also set to the very concept of recoverable damages. Indeed, under art. 9 PLD the producer is only liable to compensate for two types of damages: those caused by death or personal injuries, and those cause to, or by the destruction of, items of property other than the defective product itself, with a lower threshold of 500 euros, provided that the former is of a type ordinarily intended for private use, or it was primarily used so by the injured person. National provisions relating to non-material damages may still apply. Moreover, art. 16 allows MS to limit liability for damages deriving from death or personal injury and caused by identical items with the same defect to a minimum of 70 million euros.

## 3.4. The Product Liability Directive: an assessment

The PLD has been subject to periodic evaluation-reports by the European Commission, aiming at assessing the effectiveness of the product liability regime, in light of its national implementation and its actual application, especially against the challenges brought about by new technologies.

The latest official evaluation[120] – as well as the study upon which it is based[121] – identified some problematic issues that may be worth revision (which will be considered in §§ 3.4.1 and ff.). However, they found the PLD overall adequate to face the challenges posed by existing and emerging products – being deemed both relevant, effective and efficient.

[120] European Commission (2018). Commission Staff Working Document. Evaluation of Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products. Brussels, European Commission.

[121] Ernst&Young, Technopolis and VVA (2018). Evaluation of Council Directive 85/374/EEC on the approximation of laws, regulations and administrative provisions of the Member States concerning liability for defective products. Brussels, European Commission.

On the basis of this considerations, the Commission appointed an Expert Group working in two formations – one dealing with the PLD itself, the other with new technologies – to evaluate the applicability of the PLD and overall liability regimes to traditional products and new technologies, and developing « guidelines for possible adaptations of applicable laws at EU and national level relating to new technologies»[122].

On November 2019 the New Technology formation published its conclusion, which will be analysed in detail in Ch. 4, § 4.6 below[123]. As we will see in the next chapter, said study focuses on liability for new technologies broadly intended, as primarily comprised by national non-harmonized contractual and non-contractual law, and thus discusses the PLD only as part of a bigger picture. A specific discussion on the matter falls within the report of the PLD formation, which, however, has not yet been made public at the time of writing.

In its assessment of existing liability regimes in the wake of emerging digital technologies, the New Technologies Formation of the Expert Group claimed that (i) the existing liability framework provided by the non-harmonized contractual and non-contractual liability ensures basic protection against damages caused by new technologies; (ii) nevertheless, certain characteristics of said technologically advanced applications may make it difficult for the victim to claim for compensation, ultimately resulting in an unfair allocation of the costs derived from technological development.

Against this background, the EG suggested a series of solutions, adjusting both national and EU regimes. As for the PLD and its national implementation, the EG further elaborated the considerations made in the latest Commission Evaluation, and proposed some modifications to make the PLD fitter to regulate liability deriving from the use of new technology, concerning, in particular, the need to: (i) expand the notion of product, (ii) to facilitate the victims burden of proof at the national level, (iii) extend the notion of commercialization as to accommodate updates in the products' lifecycle, (iv) to exclude the development risk defence[124].

However, assessing the relevance, effectiveness and efficiency of the PLD ultimately implies evaluating to what extent it fulfils the objective it was designed for.

Firstly, despite the «maximum harmonization» realised by the PLD for product liability claims, significant differences remain in the product liability regime across MS. Indeed, the directive itself allows for some degree of discretion in its implementation, as far as both the scope of application and the substantive disciplines are concerned[125].

As a mere example, it may be recalled that Germany enacted both the *Gesetz über die Haftung für fehlerhafte Produkte* (ProdHaftG)[126] as general legislative framework, as well as providing liability specifically for given technologies, such as the *Gesetz zur Regelung der Gentechnik*, or the *Atomgesetz*,

[122] See in this respect https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3592 (last accessed June 29th 2019).

[123] Expert Group on Liability and New Technologies - New Technology Formation (2019). Report on Liability for Artificial Intelligence and other emerging digital technologies.

[124] Ibid.; European Commission (2020). Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee. Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, European Commission., 5ff.

[125] Again, for an overview see Machnikowski, P. (2016). European Product Liability. An Analysis of the State of the Art in the Era of New Technologies. Cambridge, Intersentia. In particular, reference to German and French legislation may be found in Borghetti, J.-S. (2016). Product Liability in France. European Product Liability. An Analysis of the State of the Art in the Era of New Technologies. P. Machnikowski. Cambridge, Intersentia: 205-236, Magnus, U. Ibid.Product Liability in Germany: 237-274.

[126] Gesetz über die Haftung für fehlerhafte Produkte vom 15. Dezember 1989 BGBl. I S. 2198.

or the *Arzneimittelgesetz*[127], while France only has one single piece of legislation that applies to all technological applications, constituting «products» under the PLD[128].

With regard to the choices allowed by art. 16 of the PLD, the *ProdHaftG* provides that, in case of death and bodily injury, a maximum amount of € 85 million is recoverable, regardless of whether the award is set to compensate several damages caused by a single defective product, or a series of products of identical terms (§ 10 *ProdHaftG*). On the contrary, French law compensates any kind of damages, but for those explicitly excluded by the directive, and no liability-cap is set.

Furthermore, the PLD sets a regime of maximum harmonization for product liability claims but leaves untouched the possibility for cases involving damages caused by defective products to be solved through other grounds of contractual or non-contractual liability, such as fault and negligence, or warranty for latent defects (art. 16 PLD). In as much as these rules constitute a significant ground for compensation – and thus play a leading role in shaping the liability of producers for the damages caused by the defect of their products – the goal of ensuring a uniform system of product liability is far from being ensured.

As for the second goal, that of achieving «a fair apportionment of the risks inherent in modern technological production» through a system of no-fault liability, a series of problematic issues may be identified, which are worthy of specific attention.

First of all, it is important to distinguish the two functional components of the aforementioned aim: the deterrent effect of liability rules, which are supposed to lead to a high standard of product safety, and their compensatory effect, which instead focuses of ensuring that producers make good for the losses caused.

As for the first component, it is questionable whether a no-fault system of liability is the «the sole means of adequately solving the problem» of risk distribution, as stated by the directive, as law and economics theories successfully showed how objective standard of liability do not lead to higher safety investments compared to those induced under a fault-liability regime, given that the producer would be forced to pay damages regardless of any safety-related cost that she may have *ex ante* internalized[129].

However, the same consideration explains why objective liability is the most adequate to ensure compensation of the victim, and thus to fulfil the second component of the «fair apportionment of the risks» that the directive aspires to achieve.

If this works on a theoretical level, the actual capacity of the directive to ensure compensation of the victim rests upon how smooth and successfully liability claims may be established in practice. This question has been directly addressed by the study which the latest official assessment of the PLD is based upon, whose primary focus is indeed empirical. As we anticipated before, the study found the directive overall relevant, effective and efficient in granting compensation to the victims of damages caused by defective products, at least as far as traditional technologies are concerned.

It grounds the alleged effectiveness of the PLD on two main justifications: the support shown by stakeholders, and the limited number of cases litigated, which instead are said to be solved in out-of-court settlements. From a methodological point of view, both of these justification seem critical. Firstly, the data collected for the purpose of the study is reached through computer assisted interviews and

[127] Gentechnikgesetz in der Fassung der Bekanntmachung vom 16. Dezember 1993 (BGBl. I S. 2066); Gesetz über die friedliche Verwendung der Kernenergie vom 23. Dezember 1959 BGBl. I S. 814; Arzneimittelgesetz in der Fassung der Bekanntmachung vom 12. Dezember 2005 (BGBl. I S. 3394); the latter, for example, set a regime of strict and absolute liability: § 84.

[128] Loi n. 98-389 of May 19, 1998, modifying the French civil code.

[129] Posner, R. (2007). Economic Analysis of Law, Wolters Kluwer., 182.

contact with a limited pool of stakeholders, namely IT representatives, legal experts and producers, which – if not adequately contrasted to opposed interests and perspectives – may be misleading. It is questionable whether consumers' participation to the public consultation suffice for the purpose[130].

Despite being aimed at assessing the adequacy and relevance of the PLD as a standalone piece of legislation, the study actually considers the application of a broader liability regime, including other pieces of legislations, such as national non-harmonized rules and rules on product conformity[131]. In as much as it does not isolate the application of the PLD, it is not capable of picturing exactly how it is capable of ensuring protection for damages caused by defective traditional and technologically advanced products. In particular, the limited number of cases litigated under the PLD against a higher caseload base on different grounds of liability may actually show that victims struggle to find protection under the directive, and rather resort to alternatives with higher degree of success[132].

Furthermore, other bodies of regulation, such as the Consumer Sales and Guarantees Directive (CSGD), which structurally offer a remedy for the user without the need to resort to in-court litigation, are at times erroneously overlapped with the PLD, often as a consequence of the confusion that interviews and participants to the public consultation have about the relationship between the two[133]. This methodological bias is even more relevant if we consider that – as the study itself acknowledges – in some cases courts have granted compensation on the basis of a different ground – be it contractual or tortious liability –, despite the claimant had actioned her rights under the PLD[134].

In the worst case scenario, rather than proving that product liability rules succeed in giving the incentives for releasing safe product onto the market – thus leading to limited accidents –, low-litigation may signal that victims are discouraged to bring a case against the producer. In other words, few claims for damages does not mean that few damages occurred.

The limited success of the PLD is to be found in a series of problematic features, which substantially diminish the victims' capacity to rely on it as a ground for damage, or to successfully prove the constitutive elements of her claim, while enabling the producer to escape liability in way that questions the very paradigm – strict and objective liability – which the PLD is based upon. Most importantly, all these problems are likely to be exacerbated in case of damages caused by technologically advanced application, such as those based on the AI elements whose features – such as connectivity, autonomy, data dependency, complexity in the supply chain, openness to continuous updates, opacity of decision making and vulnerability to cyber threats – significantly challenge the viability and application of existing rules[135].

[130] Timan, T., R. Snijders, M. Kirova, S. Suardi, M. v. Lieshout, M. Chen, P. Costenco, E. Palmerini, A. Bertolini, A. Tejada, S. v. Montfort, M. Bolchi, S. Alberti, R. Brouwer, K. Karanilokova, F. Episcopo and S. Jansen (2019). Study on safety of non-embedded software. Service, data access, and legal issues of advanced robots, autonomous, connected, and AI-based vehicles and systems: final study report regarding CAD/CCAM and industrial robots. Brussel, European Commission. ibid.

[131] Directive 1999/44/EC of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees.

[132] Indeed, the cited report highlights that «even if the Product Liability Directive and the contractual liability legislation have different but complementary scopes, often clients do not know the difference between the Product Liability Directive and the guarantee».

[133] The report itself highlights that «even if the Product Liability Directive and the contractual liability legislation have different but complementary scopes, often clients do not know the difference between the Product Liability Directive and the guarantee», where the guarantee is that offered by the CSGD, art. 3 and art. 6: Ernst&Young, Technopolis and VVA (2018). Evaluation of Council Directive 85/374/EEC on the approximation of laws, regulations and administrative provisions of the Member States concerning liability for defective products. Brussels, European Commission., 56.

[134] Ibid.22: «it also appears that claimants sometimes invoked the national law implementing the Directive as main law, but the courts allowed for compensation on a different legal basis, either tort or contract law, in around 20% of the cases. In those cases, on average, the legislation allowing the injured persons to raise a claim was contract law in 68% of the cases, general tort law in 21% of the cases».

[135] European Commission (2018). Commission Staff Working Document. Evaluation of Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products. Brussels, European Commission. Machnikowski, P. (2016). European Product Liability. An Analysis of the State of the Art in the Era of New

### 3.4.1. Notion of product and distinction with services: the issue of software

One of the major obstacles for a case to be successfully actioned under the PLD, is that the device whose defect caused a damage may not be considered a «product», but rather a «service», and thus falls outside the scope of application of the directive.

If this limited scope might not have been too problematic when the directive was enacted, the distinction between product and services, and the exclusion of the latter from its scope of application is now becoming a major issue. Indeed, the PLD was designed with a traditional, tangible, movable and mass-produced product in mind.

So far, the Court of Justice indicated that the PLD applies to products used while providing any service, and thus partially extended the application of the directive. However, it clearly stated that liability of a service provider does not fall within the scope of the directive[136].

A second and related issues is whether the notion of product should be interpreted as to include software, or whether the latter shall be qualified as a service, thus falling – absent the element of embedment into a tangible product – outside the scope of application of the PLD. This uncertainty represents a major problem, as the technologically advanced applications often display both software and hardware elements, which are tightly connected in their functioning (e.g. as in the case of connected and automated driving solutions, where the self-driving features represents the novel aspect of the application, differentiating it from traditional vehicles), while in other cases rely exclusively on non-embedded algorithms and AI-based solutions (e.g. computer programs which could be downloaded or used over the cloud)[137].

If distinguishing products from services – e.g.: in a mobility-as-a-service scenario – might be sensible – despite being sensible to hold both the producer and service producer responsible, yet on different grounds (see Ch. 5 §§ 5.1-5.2) – distinguishing software from other material products may not.

### 3.4.2. Notion of defect

Product liability covers damages caused by defects in a product.

However, understanding what constitutes a «defect» under the PLD may be problematic. Since the defective or safe nature of a product is also expressly connected to the reasonable expectations of the consumer, it is likely that disputes will emerge regarding the degree of safety that the consumer may expect, and whether a certain misuse should have the reasonably anticipated and thus accounted for by the producer. In as much as this type of assessment implies an evaluation of the design and presentation of the product, also *vis a vis* particular types of perspective users (e.g. vulnerable subjects such as children or the elderly), the notion of defect leads to a subtle shift from an objective to a fault-based liability, despite only the first one is considered by the directive adequate for a fair apportionment of the risks of production.

Furthermore, demonstrating defectiveness may in itself be burdensome – especially in case of design-defects –, and may require data and technical skills which the victim might not possess. This is an even

Technologies. Cambridge, Intersentia, Expert Group on Liability and New Technologies - New Technology Formation (2019). Report on Liability for Artificial Intelligence and other emerging digital technologies.

[136] See in this respect CJEU, Judgement of 21 December 2011, Case C-495/11, Dutrueux and Caisse primaire d'assurance maladie du Jura. The same perspective is shared by the EG, Technologies, 28, and Timan, T., R. Snijders, M. Kirova, S. Suardi, M. v. Lieshout, M. Chen, P. Costenco, E. Palmerini, A. Bertolini, A. Tejada, S. v. Montfort, M. Bolchi, S. Alberti, R. Brouwer, K. Karanilokova, F. Episcopo and S. Jansen (2019). Study on safety of non-embedded software. Service, data access, and legal issues of advanced robots, autonomous, connected, and AI-based vehicles and systems: final study report regarding CAD/CCAM and industrial robots. Brussel, European Commission., 145.

[137] Expert Group on Liability and New Technologies - New Technology Formation (2019). Report on Liability for Artificial Intelligence and other emerging digital technologies., 28.

greater issue for technologically complex products that are meant to operate in a highly-interconnected digital ecosystem. In the case of an autonomous vehicle's sensor, the victim may not be in the condition to know whether the sensor didn't work because of an internal malfunctioning (e.g. defective installation of the camera, leading to partial view of the street), or whether they operated correctly, and simply didn't work for other reasons, such as e.g. a lack of connectivity, the another subject – the network provider – was supposed to ensure[138] (on the different, yet related issue of the establishment of the causal nexus, see § 3.4.4 below).

### 3.4.3. Development risk defence

Most importantly, even if the operation of the device may be considered a defect pursuant to art. 2 PLD, the defences under art. 7 PLD and – in particular, the so called «development risk defence»–, may allow manufacturers to escape liability.

While the majority of the exclusionary circumstances is intended to prove that the producer has not integrated the conduct which triggers the liability regime (e.g. she did not put the product into circulation; the defect did not exist at the time when the product was put into circulation, or that it came into being afterward; etc.) the specific cause under art. 7(e) departs significantly from this paradigm. Indeed, under the development risk defence, the producer may avoid liability if the state of scientific and technical knowledge at the time the product was put into circulation was not such as to enable the existence of the defect to be discovered.

Liability without fault is «the sole means» of ensuring victim's compensation. Nevertheless, the development risk defence introduces an element of negligence, since the manufacturer who met the state of the art of scientific development and technological advancement may not be blamed when, nonetheless a harmful event resulted from the use of his product. By doing so, the development risk defence ultimately frustrates the ideal of a strict liability which the directive commits to.

### 3.4.4. Causal nexus

Against this background, ascertaining the causal nexus between the defect and the damage may be equally hard[139]. Determining that harm is the consequence of a defect in the functioning of the device requires an in-depth analysis of the product and of its functioning, which, in turn, presupposes relevant technical expertise. The more technologically complex the product is, the more difficult it will be to precisely identify and prove that a given defect was indeed the reason why a specific damage occurred.

For example, self-driving cars with high degree of automation are meant to combine autonomous and traditional driving modes, so that the car might even require the human pilot to resume control under different circumstances, including possible system failures. Even if the consumer manages to prove that some element of the car (e.g. its sensors) was defective, it may be disputable whether the accident was caused by the failure of the system, or rather by the incapacity of the driver to take back control when requested to. Most likely, the producer will advocate that the failure of a specific element of the car was not in itself a defect, because the car was programmed to adjust to such malfunctioning

[138] Timan, T., R. Snijders, M. Kirova, S. Suardi, M. v. Lieshout, M. Chen, P. Costenco, E. Palmerini, A. Bertolini, A. Tejada, S. v. Montfort, M. Bolchi, S. Alberti, R. Brouwer, K. Karanilokova, F. Episcopo and S. Jansen (2019). Study on safety of non-embedded software. Service, data access, and legal issues of advanced robots, autonomous, connected, and AI-based vehicles and systems: final study report regarding CAD/CCAM and industrial robots. Brussel, European Commission., Annex 3, Task 3&4, 131-150.

[139] See Expert Group on Liability and New Technologies - New Technology Formation (2019). Report on Liability for Artificial Intelligence and other emerging digital technologies., ibid. especially 28. Ernst&Young, Technopolis and VVA (2018). Evaluation of Council Directive 85/374/EEC on the approximation of laws, regulations and administrative provisions of the Member States concerning liability for defective products. Brussels, European Commission.

disabling the autonomous driving mode, and that – in any case – it was not the original malfunctioning that caused the damage, but rather the way the driver responded to the situation.

Thus, the victim may not succeed in proving the constitutive elements of his claim in light of complex interaction of multiple elements susceptible to influence and shape the causal nexus alternatively. In the worst case scenario, the limited expectation of success and the perspective of high-litigation costs may dissuade the consumer from filing a claim all together, especially in case of low-value disputes.

The EG extensively discusses the evidentiary-burden issues, and rightfully comes to the conclusion that the current system is suboptimal and should be revised to the benefit of the victim. The Report clearly allocates this problem at the national law level, as the directive rests on national procedural rules[140]. However, as we will see in § 3.6 below, the need for a high standard of harmonization would rather suggest that such revision be made directly at the European level, substituting the allocation of the burden of proof in art. 4 PLD.

### 3.4.5. Recoverable damages

Finally, it is worth mentioning that technologically advanced applications may render the very notion of recoverable damages – as defined in the PLD – inadequate for ensuring effective compensation.

As illustrated in § 3.33.3 above, three types of limits shape the award granted to the victims under product liability rules.

Firstly, only damages caused by death or personal injuries, and those caused to, or by the destruction of, items of property other than the defective product itself, with a lower threshold of 500 euros, may be compensated; however, MS may still apply rules allowing the recovery of non-material-damages. Secondly, said damages must have been caused by a product that was ordinarily intended for private use, or that was primarily used so by the injured person. Finally, art. 16 allows MS to limit liability for damages deriving from death or personal injury and caused by identical items with the same defect to a minimum of 70 million euros.

Given the vast variety of interests involved, the current limitation to physical and material damages may be questionable, especially in as much as it does not address privacy and cybersecurity issues. Other problems may be connected to the non-harmonized solutions available for the recovery of non-material damages, which the directive specifically leaves to MS to address, as well as to loss of data, since no clear definition of the latter is available at EU level and MS may qualify it as property or not depending on their specific policy interests[141].

Furthermore, the limitation under art. 9 implies that damages caused to the product themselves are non-recoverable. In the best case scenario, the consumer may be able to receive some form of relief for this type of damage, on the basis of other grounds of national tort or contractual law, or by reference to the CSGD, which, however, is based on the different presumption of the lack of conformity, and is subject to stringent statutes of limitation and denunciation rules.

This limitation is understandable in the original context in which the directive was meant to operate, where product liability rules were considered rules of occasional application, covering damages caused by products, whose value was often relatively low, at least compared to the other interests infringed (e.g. a hairdryer, whose faulty electric systems causes it to catch fire, causing serious physical injuries to its user). With the advancement of new technologies and, in particular their autonomous and often

[140] Expert Group on Liability and New Technologies - New Technology Formation (2019). Report on Liability for Artificial Intelligence and other emerging digital technologies., 28, 30 and *passim*.

[141] Ibid.

unsupervised functioning, replacing human operators, the range of application of the PLD will expand to include cases that today fall outside its scope. If no human is in direct control, most likely damage will depend upon the functioning of the device itself, thence liability for defective products might be looked at to ensure compensation even in claims of more frequent occurrence, and lesser value that today are instead the elective domain of the general rules of liability applicable ordinarily in tort (e.g. in the case of a self-driving car that crashed into another car due to a defect of its sensors, merely denting its bumper, with no other significant damage to the rest of the car).

In such cases, damages to the defective product itself might be relevant both in absolute – for the value of the device might be conspicuous –, and relative – to other damages suffered – terms. At the same time, the cost of litigation, primarily due to the complexity of the claim might be disproportionate with respect to the damage suffered.

## 3.5. Towards a reform of the Product Liability Directive

Against this background, the current status of the EU product liability regime needs to be re-shaped to better address the challenges brought about by new technologies.

First of all, the PLD rules should be revised as to better ensure a fair distribution of risks among the various subjects involved.

In the light of what we said in § 3.3 above, this goal should be intended as limited to ensuring effective compensation, without including considerations directed to incentivise, through liability rules, high level of safety investments.

In general terms, civil liability rules pursue three functions: the first and most important one is the *ex post* compensation of the victim, as they force the person responsible for the damage to make good for the loss suffered. Furthermore, they also ensure *ex ante* deterrence, as they make it economically inefficient for the agent to realize the harmful conduct, and thus incentives positive behaviours. Finally, and to a more limited extent, they may also function as *ex post* punishment in the sense that if ensures that the infringer does not get away with the illicit behaviour. This is particularly true in case of disgorgement or punitive damages, which aims to strip the infringer from the gains made through the harmful conduct or to punish particularly reprehensible conducts. However, there is a very limited availability of this types of damages under European law, where civil remedies are mostly directed to ensure compensation and react to the infringement in an effective, dissuasive and proportional way.

These functions relate to each other differently and may be balanced according to different equilibrium. Most importantly, while the compensatory aim stands out as the characteristic function of civil liability, both deterrence and punishment maybe me seen as «incidental» effects of the compensatory awards, as well as «additional» functions, which may be achieved by structuring liability rules (standard of liability, limits of the award etc. etc.) in a particular way.

Indeed, it may very well be that deterrence and punishment are better achieved through a cap. In such a perspective, product safety is best achieved through narrow tailored *ex ante* regulation detailing relevant safety requirement. Once deterrence and compensation are decoupled, and product liability may be directed solely towards the second aim, the specific regime of the PLD should be evaluated and revised as to maximise its capacity to ensure full compensation to the victims[142].

[142] Bertolini, A. (2014). Robots and liability - Justifying a change in perspective. Rethinking Responsibility in Science and Technology. F. Battaglia, J. Nida-Rümelin and N. Mukerji. Pisa, Pisa University Press: 143-166, Palmerini, E. and A. Bertolini (2016). Liability and Risk Management in Robotics. Digital Revolution: Challenges for Contract Law in Practice. R. Schulze and D. Staudenmayer. Baden-Baden, Nomos: 225-259. Bertolini, A. (2014). Robots and liability - Justifying a change in perspective. Rethinking Responsibility in Science and Technology. F. Battaglia, J. Nida-Rümelin and N. Mukerji. Pisa, Pisa University Press: 143-166, Palmerini, E. and A. Bertolini (2016). Liability and Risk

In particular, a revision of the PLD should aim at overcoming those inefficiencies and puzzles that:

(i) limit the scope of application of the directive (i.e. the fact that is does not cover damages caused by software, unless the latter is meant to be addressed through a different and specific regulation);

(ii) burden the position of the victim, by requiring her to prove both the damage suffered, the defect, and the causal nexus between the two, often without any duty of disclosure of relevant information on the side of the producer;

(iii) compromise the strict liability paradigm adopted by the directive (i.e. reference to the standard of «reasonableness» in the notion of defect, and negligence-based assessment enshrined in the development risk defence).

As it will be further discussed in Ch. 5, a possible solution to these issues could be that of framing product liability according to a Risk-Management-Approach (RMA), which allocates the duty to compensate damages on the party who profits from the dangerous activity since she is best positioned to manage risks by spreading them onto all users of the same product. Pursuant to this approach, it is also essential to identify one clear and certain entry point for all litigation (one-stop-shop) to minimize the costs of access to justice for the victim and increase her chances of obtaining compensation (reducing risks of alternative causation - see Ch. 4 § 4.7.3) (§ 5.2).

Finally, it is indeed questionable whether product liability rules could be constructed in a technological neutral way, as the PLD intends to do. On the contrary, liability rules should be developed according to a bottom-up, functional and thus sector specific approach, providing narrow tailored solutions to application-specific problems[143]. In particular, legal rules should correspond to three main features, namely:

(i) the specific technical features of given classes of applications;

(ii) the specific features of the perspective users (business-users, general public, experts, etc.);

(iii) the specific features of the relevant market, including the availability of insurance.

In this sense, the PLD may qualify as a general rule, covering both traditional products and new technologies. However, for the latter it should play a residual role – similarly to the one performed by the GPSD in the product safety regulation –, while narrow tailored regulations should be adopted at the European level, for specific classes of applications, as to meet the social and legal challenges that each one gives rise to (§ 5.3).

## 3.6. Ensuring a high standard of harmonization.

Finally, the PLD shall be revised as to ensure a high standard of harmonization.

As we recalled in above, one of the directive's aim was precisely that of «approximation of the laws of the member states concerning the liability of the producer for damage caused by the defectiveness of his products […] because the existing divergences may distort competition and affect the movement of goods with the common market and entail a differing degree of protection of the consumer against damage caused by a defective product to his health or property».

---

Management in Robotics. Digital Revolution: Challenges for Contract Law in Practice. R. Schulze and D. Staudenmayer. Baden-Baden, Nomos: 225-259.

[143] On the functional approach to technology regulation, see Palmerini, E., F. Azzarri, F. Battaglia, A. Bertolini, A. Carnevale, J. Carpaneto, F. Cavallo, A. Di Carlo, M. Cempini, M. Controzzi, B.-J. Koops, F. Lucivero, N. Mukerji, L. Nocco, A. Pirni, H. Shah, P. Salvini, M. Schellekens and K. Warwick (2014). Guidelines on Regulating Robotics. Robolaw Grant Agreement Number: 289092, D6.2.

This aim is frustrated by the very structure of the directive, which – while providing maximum harmonization on product liability claims – it allows MS to keep or introduce new claim for damages based on grounds of contractual liability or on grounds of non-contractual liability other than that provided for in this directive. Empirical evidence has proved that, in light of the insufficient protection afforded by the directive to victims of damages caused by defective products, a relevant number of the cases which would theoretically fall within the scope of application of the PLD, are actually litigated on different grounds, according to national contractual and non-contractual rules[144].

The reliance on non-harmonized systems of protection, thus, hinders the creation of that level playing field in consumer protection and business competition that the PLD strives to achieve.

Moreover, such scenario may critically hinder the creation of a common market of technological products in the EU. Indeed, legal rules are not neutral as far as technological advancement is concerned, as different regimes may lead to the development of different products and alternative solutions among possible alternatives, which better accommodate the incentives provided. Therefore, were advanced technologies regulated at MS level, differences would not only cause legal fragmentation, but also the market's, leading to different kinds of technologies to be developed[145].

Since legal rules determine what kind of technological application is favoured over others – and thence they are not technology-neutral – uniformity across MS is essential.

[144] «It also appears that claimants sometimes invoked the national law implementing the Directive as main law, but the courts allowed for compensation on a different legal basis, either tort or contract law, in around 20% of the cases. In those cases, on average, the legislation allowing the injured persons to raise a claim was contract law in 68% of the cases, general tort law in 21% of the cases», Ernst&Young, Technopolis and VVA (2018). Evaluation of Council Directive 85/374/EEC on the approximation of laws, regulations and administrative provisions of the Member States concerning liability for defective products. Brussels, European Commission., 22.

[145] With specific reference to self-driving cars, Bertolini, A. and M. Riccaboni (2018). The Regulation of Connected and Automated Driving. A Law and Economics Analysis of Liability Rules. W. Paper.

# 4. A EUROPEAN APPROACH TO LIABILITY FOR AI-BASED APPLICATIONS

### Distinction between low- and high-risk AI, and liability implications

31. The distinction between low- and high-risk AI-based applications based on the notion of «significant harm» as advanced by the EG is impossible to determine, due to lack of statistically relevant data on the size and frequency of expected damages [§ 4.6.3].
32. Similarly, this distinction is based on questionable criteria, such as the economic relevance of the claim and the public-space operation of the AI- systems. Other criteria instead are not considered [§ 4.6.3]
33. Excluding strict liability for smaller claims – falling under the notion of low-risk – leads to inefficiencies and denied justice for many parties, in particular those that might be rooted in the every-day use of advanced technologies [§ 4.6.3].
34. Likewise, whether a technology is operated in the private or public space is not of primary importance in determining the level of risk a given application gives rise to, and subsequently the need to regulate it through strict liability rules (expert systems operate in private environment and may raise significant risks, requiring ad hoc intervention) [§ 4.6.3].

### Reliance on MS procedural rules. Logging by design

35. Relying on the reversal of the burden of proof at MS level, operated by courts implementing well-established doctrines (e.g.: *res ipsa loquitur*) is insufficient [§ 4.6.4].
36. Logging by design is useful but insufficient to ensure the possibility of the victim to establish the liability of the producer/operator/deployer. Elaborating data and interpreting it is a complex and costly activity and the claimant might not possess the capacity or the incentives to do it, discouraging access to justice and damage compensation [§ 4.6.5].

### Regulating technology at EU level: competence

37. The EU should regulate advanced technologies, seeking maximum harmonization among MS, and should intervene through regulations rather than directives towards that end. Different implementations could lead to excessive market fragmentation [§ 4.7 & § 4.7.1].
38. The EU possess the necessary competence for such kind of initiatives [§ 4.7 & § 4.7.1].

### A technology-specific approach

39. The EU should not attempt to regulate «AI-based technologies» unitarily even with respect to liability. Using broad umbrella notions such as «AI-systems» causes regulation to be both under- and over-inclusive, encompassing too diverse applications, many of which require no legal intervention [§ 4.7.1].
40. The EU should pursue continuity in its sectorial approach to regulation. There is no need for a uniform regulation of all AI-based applications, not even with respect to liability. AI is pervasive, it is and will be used in diverse fields, including but not limited to medical diagnosis, capital markets, consumer products and services, industrial production, energy production and distribution. As even liability aspects are, for the most part, separately regulated, so they should continue to be separately regulated when AI-based solutions are implemented [§ 4.7.2].
41. A technology-specific approach to the regulation of AI better conforms to the principles of proportionality and subsidiarity, minimizing risks of undesirable interferences with MS legal systems, and is in line with the «better regulation» guidelines Adopted by the European Commission in 2017 [§, 4.7.1, § 4.7.7].

42. Only those applications that pose relevant legal and social concerns and according to a complex assessment that takes into account the overall legal framework specifically applicable to them, should be regulated [§ 4.7.4].

**Ensuring victim compensation, the need for a single entry point for litigation**

43. The legal system should primarily seek victims' compensation in all cases where the victim is not responsible for the harm suffered. When victims fail to obtain compensation, and they are not themselves responsible for the harm suffered, that is a failure of the legal system that policy-makers should attempt to overcome by reforming existing regulation [§ 4.7.3].
44. «Alternative causation» is a serious concern when advanced technologies are considered. These will in fact require the cooperation of multiple parties in their operation and use. Alternative causation in damages caused by advanced technologies could lead to frequent victims' undercompensation. In such scenarios it may be impossible to identify the responsibility of one single party among multiple potential tortfeasors [§ 4.7.3].

**A single entry point for litigation, and the need for a clear responsible party**

45. Access to justice and victims' adequate compensation is best ensured by identifying a clear responsible party among the different potential tortfeasors (one-stop-shop) [§ 4.7.4].
46. The party to be held liable should be the one that is best positioned to (i) identify, (ii) control and (iii) manage the risk, irrespective of considerations of fault [§ 5.1] (strict or absolute liability rules).
47. The single *prima facie* responsible party towards the victim should be granted rights to sue in recourse those parties that contributed to causing the harm [§ 4.7.4].
48. Contractual agreements among the parties distributing responsibility along the value chain should be favoured [§ 4.7.4].
49. Who, among the possible responsible parties – producer, owner, user, business user, operator –, ought to be held responsible should be assessed with respect to the specific class of applications the legislator intends to regulate. Only one party should be *prima facie* liable towards the claimant [§ 4.7.4].
50. Damage caps should be specific for a given class of applications for general caps might be inadequate as excessively high or low for some specific cases. Damages should in fact always pursue a compensatory function, and should therefore be proportionate to the real harm suffered, even when limited [§ 4.7.6] .
51. It is not advisable to exclude certain categories of damages from compensation (e.g. non-pecuniary losses). MS have different approaches, and law considerations, some of which rooted in constitutional law considerations and an EU intervention could conflict with some of them [§ 4.7.6].

## 4.1. Defining a European approach through three ideas

Regulating advanced technologies is a challenge for Europe[146]. The global competition for their development, deployment, and use, with the subsequent economic and social impact they will bring about[147], calls for a coordinated intervention at supranational level, that is not only respectful but also shaped by the European approach characterized by the utmost respect for fundamental rights, and user's protection, while promoting economic development.

Said principle is clearly mentioned in all European political statements touching upon advanced technologies and their regulation[148]. However, with respect to civil liability, it shall be further specified in three different ideas – that should shape initiatives aimed at reforming the subject matter – , the need:

(i) for a European solution, that does not primarily resort to MS' pre-existing legislation, in particular in terms of general principles of liability in tort or contract law (see § 4.2 below);
(ii) to rethink the liability paradigm, also overcoming the existing and applicable one, provided for by the PLD;
(iii) to pursue the highest level of protection for the user and potential victim, possibly improving their conditions.

## 4.2. Going beyond MS' civil liability regulation: seeking uniformity

The EG acknowledges that harmonization at European level with respect to liability rules is limited, and even when it comes to the PLD – by far the most relevant body of regulation applicable to advanced technologies, according to the paradigm described in the previous chapters – «[…] efforts to overcome such differences [among MS] by harmonizing only certain aspects of liability law may not always lead to the desired degree of uniformity in outcomes»[149].

Similarly, the European Commission in its most recent statement stressed how «[…] the characteristics of emerging digital technologies like AI, the IoT and robotics challenge aspects of Union and national liability frameworks and could reduce their effectiveness. Some of these characteristics could make it hard to trace the damage back to a human behaviour, which could give grounds for a fault-based claim in accordance with national rules […]»[150].

Both statements are correct, in that they precisely describe the *status quo*. Insufficient harmonization at European level will, in fact, lead to (i) insufficient users' protection, and (ii) market fragmentation,

[146] Bertolini, A. and E. Palmerini (2014). Regulating Robotics: a Challenge for Europe. Upcoming Issues of EU Law, available at http://www.europarl.europa.eu/document/activities/cont/201409/20140924ATT89662/20140924ATT89662EN.pdf. D.-G. f. I. Policies. Bruxelles.

[147] OECD (2017). The Next Production Revolution. and Dachs, B. (2018). The impact of new technologies on the labour market and the social economy Brussels, STOA.

[148] Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics COM(2020) 64 final, European Commission, White Paper - On Artificial Intelligence - A European approach to excellence and trust COM(2020) 65 final Brussels, European Commission, Kritikos, M. (2016). Legal and ethical reflections concerning robotics, STOA Policy Briefing. June 2016-PE 563.501, available at https://www.europarl.europa.eu/RegData/etudes/STUD/2016/563501/EPRS_STU(2016)563501(ANN)_EN.pdf. European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL), (2019). European Parliament resolution of 12 February 2019 on a comprehensive European industrial policy on artificial intelligence and robotics (2018/2088(INI)), European Parliament. European Commission (2017). SWD(2017)350. Commission Staff Working Document. Better Regulation Guidelines. Brussels.

[149] Expert Group on Liability and New Technologies - New Technology Formation (2019). Report on Liability for Artificial Intelligence and other emerging digital technologies., 16.

[150] Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics COM(2020) 64 final, European Commission., 13.

ultimately (iii) affecting the proliferation and diffusion of desirable technologies and its connected industry[151] (see Ch. 5, §§ 5.5.3 and 5.7.2).

Liability rules not only determine who bears the economic consequences of an accident – the victim who fails to achieve compensation, the owner of the application being used, its designer or producer or distributor, the service provider or possible third parties, upon which a vicarious liability might be established – but also shape incentives for all parties involved. This encompasses both technology development and adoption. Liability rules affect product design, as well as the rational choice to adopt a more technologically advanced solution over a more traditional one.

EU policy makers are aware of said effect of regulation on technological development, and actually rightfully pursue it and exploit it, by introducing «by-design» requirements in order to ensure users' rights are respected.

In such a framework, uniform regulation appears essential. Thence, the circumstance that currently all MS' legal system would be able to provide a solution to liability issues arising from the use of advanced technologies does not in itself entail that no intervention by EU institutions is needed. Quite the contrary, prompt regulation pursuing higher degrees of harmonization than those achieved currently by the PLD appears to be necessary.

While, indeed, MS have not yet regulated advanced technologies unitarily[152], some piecemeal interventions are starting to emerge, for instance with respect to automated driving solutions[153], and some specific applications are instead already regulated in quite some detail, despite, in some cases, with increasing degrees of uniformity[154]. Should MS intervene, adopting national legislations that would reflect divergent approaches and, at the same time, establish path-dependencies, the fragmentation of the European market for technologically advanced products would most likely result, to the disadvantage of both users – exposed to different levels of protection – and enterprises, having to comply with different standards and approaches, potentially leading to different design requirements[155].

[151] See in this respect ibid. whereby the EC acknowledges that: «should Member States eventually address the challenges to national liability frameworks, it could lead to further fragmentation, thereby increasing the costs of putting innovative AI-solutions and reducing cross-border trade in the Single Market. It is important that companies know their liability risks throughout the value chain and can reduce or prevent them and insure themselves effectively against these risks».

[152] Some interventions have instead long been discussed. Thus, in 2017 Estonia launched public discussions on the possibility of adopting an autonomous driving specific legislation – see in this respect https://e-estonia.com/artificial-intelligence-is-the-next-step-for-e-governance-state-adviser-reveals/ (last accessed June 29th 2020). Later, Estonia decided to abandon a sector-specific approach on regulating AI and is currently resorting on a general AI legal framework approach to be obtained by amending current legislation. See in this respect Ernst&Young (2019). Report of Estonia's AI Taskforce Ministry of Economic Affairs, Government Office., 38. Similarly, as part of its national strategy in the field of AI, France adopted LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique (1) which «enshrines the sequence of production, dissemination and circulation of data as a lever of growth for innovative companies and an essential driver of development in AI»; see in this respect https://www.gouvernement.fr/en/franceia-the-national-artificial-intelligence-strategy-is-underway (last accessed June 29th 2020).

[153] Timan, T., R. Snijders, M. Kirova, S. Suardi, M. v. Lieshout, M. Chen, P. Costenco, E. Palmerini, A. Bertolini, A. Tejada, S. v. Montfort, M. Bolchi, S. Alberti, R. Brouwer, K. Karanilokova, F. Episcopo and S. Jansen (2019). Study on safety of non-embedded software. Service, data access, and legal issues of advanced robots, autonomous, connected, and AI-based vehicles and systems: final study report regarding CAD/CCAM and industrial robots. Brussel, European Commission., 139-142.

[154] This is the case of civil liability for drones, on which please allow the reference to Bertolini, A. (2018). Artificial Intelligence and civil law; liability rules for drones. Brussel, European Parliament., 22-28.

[155] This is the case in the UK and Germany which have adopted ad-hoc legislation applicable to automated driving. For example, on the one hand, the enacted regulation in the UK burdens the owner of the vehicle with a duty to install safety-critical updates and the failure to do so will result in insurer's proportional limitation of liability. On the other hand, the enacted regulation in Germany holds the driver of a highly automated vehicle liable for failure to supervise the driving task, and resume control when needed. See in this respect Timan, T., R. Snijders, M. Kirova, S. Suardi, M. v. Lieshout, M. Chen, P. Costenco, E. Palmerini, A. Bertolini, A. Tejada, S. v. Montfort, M. Bolchi, S. Alberti, R. Brouwer, K. Karanilokova, F. Episcopo and S. Jansen (2019). Study on safety of non-embedded software. Service, data access, and legal issues of advanced robots, autonomous, connected, and AI-based vehicles and systems: final study report regarding CAD/CCAM and industrial robots. Brussel, European Commission., Annex 3, 139-142.

There is no doubt that the European Union possesses competence and adequate legal grounds to intervene in this subject matter with legislation that enables the highest standard of harmonization.

An intervention in such field does not need to take the direction of a profound harmonization of MS' tort and contract law systems. The perspective of the creation of a uniform – if not unified – European civil code has long been discussed, and a number of attempts have been made with broader and narrower scopes in the field of liability, as well as of obligations and contracts more specifically[156].

A more limited approach could both entail the adoption of *ad hoc* legislation or, given the qualification of machines as products – despite with uncertainties persisting with respect to software, and non-embedded AI applications whose qualification as products for the purposes of the PLD might be debated (see Ch. 3, § 3.4.1 above) – a revision of the PLD, despite the its recent positive evaluation by the Commission[157].

The first solution is preferable, for the PLD displays some structural limitations that may not be easily overcome, despite its reform might appear an altogether easier solution, requiring more limited adaptations.

## 4.3. Going beyond the Product Liability Directive: applying technology neutrality correctly

As discussed above (see Ch. 3, § 3.4), legitimate doubts arise when considering the adequacy of the PLD with respect to the challenges posed by emerging technologies, for it is largely agreed[158] that (i) the burden of proof for the claimant might be hard to meet, in particular with respect to the (ii) causal nexus, as well as the (iii) demonstration of a – most commonly design – defect, (iv) the possibility for the defendant to escape liability on the grounds of the development risk defence, and – we shall add – (v) limitations to the damages that may be compensated. Moreover, (vi) the very qualification of many advanced technologies – in particular software based ones – as product is disputable, and yet the neat distinction between products and services appears to be questionable if used to exclude those, and ultimately artificial, given the current evolution of business models through which many goods and services are provided[159].

On the one hand, the widespread agreement about the need to reform such points should suffice *per se* to deny the adequacy of the PLD itself to face the challenges posed by emerging technologies, ultimately contradicting the conclusion reached by the EC itself, stating that «the Directive is seen as coherent with the EU legislation protecting consumers, relevant and future-proof [...]»[160]. Indeed, if those aspects where addressed and changed, the very rationale and functioning of the directive would be radically modified, to an extent that while eventually bearing the same name, the new emerging piece of legislation would be rooted on other grounds, and achieve very different results. Said

[156] On this matter, see European Group on Tort Law (2006). Principles of European Tort Law. Text and commentary. Vienna, Springer; Bar, C., E. Clive and & Research Group on the Existing EC Private Law. (2009). Principles, Definitions and Model Rules of European Private Law Draft common frame of reference (Dcfr) (Full ed.). Munich, Sellier European Law.

[157] European Commission (2018). Commission Staff Working Document. Evaluation of Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products. Brussels, European Commission.

[158] Expert Group on Liability and New Technologies - New Technology Formation (2019). Report on Liability for Artificial Intelligence and other emerging digital technologies.27-28 and 42-43.

[159] Ibid., 28.

[160] See European Commission (2018). Commission Staff Working Document Evaluation of Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products SWD(2018) 157 final Brussels, European Commission., 69, and Ernst&Young, Technopolis and VVA (2018). Evaluation of Council Directive 85/374/EEC on the approximation of laws, regulations and administrative provisions of the Member States concerning liability for defective products. Brussels, European Commission., 125.

otherwise, what is portrayed as a mere adaptation of the system would instead entail a profound alteration of those equilibriums that are today affirmed as being adequate.

If we wanted to «pierce the policy veil» we could, therefore, conclude that such changes would most likely entail adopting an equivalent form to the RMA, described below (see Ch. 5, §§ 5.1-5.3).

Now, while a reform of the PLD is certainly advisable, in particular in a functional perspective that acknowledges its shortcomings as they emerged after over 30 years from its original implementation, and as they are witnessed from the empirical data collected[161] about its application across MS (see Ch. 3, § 3.4 above), the solution to the problems posed by advanced technologies is most likely better achieved otherwise, through CbC solutions.

Indeed, many commentators[162], including the EG[163] acknowledge the impossibility of elaborating a one-size-fits-all solution. Yet, proposed alternatives typically try to establish a general principle – such as the responsibility of the producer, and or operator (back- or front-end)[164] – that are again intended to be applied across categories, ultimately contradicting the original statement.

These solutions, in fact, share with the PLD a specific declination of the technology-neutral approach, that *per se* is commendable, and yet needs to account for some intrinsic limitations[165].

Technology neutrality is a principle that has a long-standing existence in the EU legal framework.

First, «technology neutrality» can be used in connection with performance standards designed to limit negative externalities posed by design standards[166]. Performance standards give regulated entities the freedom to choose the technology best suited to achieve the outcome specified, as opposed to design standards which incorporate technological choices made by the regulator[167]. This function of technology neutrality is being used under the EU data protection framework that sets forth the principle of privacy-by-design, and which states that «the protection of natural persons should be technologically neutral and should not depend on the techniques used»[168].

Second, technology neutrality is used with the aim to offer functional equivalence in the sense that «the fundamental rules should be the same online as off-line (or more broadly, the same for an online technology activity as for the equivalent off-line technology activity»[169]. This functional-equivalent approach as a separate objective of technology neutrality is being employed in the UNCITRAL Model Law on Electronic Commerce (1996) – which is the first legislative text to adopt the principles of

---

[161] See in this respect Ernst&Young, Technopolis and VVA (2018). Evaluation of Council Directive 85/374/EEC on the approximation of laws, regulations and administrative provisions of the Member States concerning liability for defective products. Brussels, European Commission.

[162] Please allow reference to Bertolini, A. and E. Palmerini (2014). Regulating Robotics: a Challenge for Europe. Upcoming Issues of EU Law, available at http://www.europarl.europa.eu/document/activities/cont/201409/20140924ATT89662/20140924ATT89662EN.pdf. D.-G. f. I. Policies. Bruxelles.and Bertolini, A. (2013). "Robots as Products: The Case for a Realistic Analysis of Robotic Applications and Liability Rules." Law Innovation and Technology 5(2): 214.

[163] Expert Group on Liability and New Technologies - New Technology Formation (2019). Report on Liability for Artificial Intelligence and other emerging digital technologies., 36.

[164] Ibid., 39-41.

[165] See in this respect European Commission (2018). Report from The Commission to the European Parliament, the Council and the European Economic and Social Committee on the Application of the Council Directive on the approximation of the laws, regulations, and administrative provisions of the Member States concerning liability for defective products (85/374/EEC). Brussels, European Commission., 34, whereby it is showed that «at the Conference on Product Liability, business associations reiterated that complex value chains and automatisation are nothing new and that the Directive is in fact technology-neutral. Only completely autonomous systems, such as self-driving cars might eventually require regulatory changes».

[166] Maxwell, W. J. and M. Bourreau (2015). "Technology neutrality in Internet, telecoms and data protection regulation." Computer and Telecommunications L. Rev. 21(1), 1–4 (2015).

[167] Ibid.

[168] See in this respect Recital 15, Recital 78 and Article 25 of the 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) OJ L 119, 4.5.2016, 1–88.

[169] Reed, C. (2007). "Taking Sides on Technology Neutrality." Script-ed 4(3)., 266.

technology neutrality and implement «media-neutral rules» – as it provides for the coverage of «all factual situations where information is generated, stored or communicated, irrespective of the medium on which such information may be affixed»[170] and lays out criteria under which electronic communications may be considered equivalent to paper-based communications[171].

Third, technology neutrality has an effect equivalence aim in the sense that legal rules should have a an equivalent effect and provide for a similar treatment across different technologies so as «to avoid limiting a right only to its exercise in extant technology or discriminating against older technology simply because it existed when the law was enacted»[172]. This concept of technology neutrality represents a cornerstone in the EU legal framework of electronic communications as the European Framework Directive 2002/21/EC imposes «the requirement for Member States to ensure that national regulatory authorities take the utmost account of the desirability of making regulation technologically neutral, that is to say that it neither imposes nor discriminates in favour of the use of a particular type of technology, does not preclude the taking of proportionate steps to promote certain specific services where this is justified, for example digital television as a means for increasing spectrum efficiency»[173].

Finally, technology neutrality is used as a legislative technique to provide future-proof regulation[174], which may survive technological development without the need of constant revisions, by providing for relevant features or characteristics rather than express categorical inclusion of specific technologies[175].

In such a perspective, while the notion of product adopted by the directive still creates a questionable distinction with services, it is still broad enough to encompass natural products, food, energy, raw materials, medical products and basically any artefact manufactured through «modern technological

[170] (1999). UNCITRAL Model Law on Electronic Commerce Guide to Enactment with 1996 with additional article 5 as adopted in 1998. New York, United Nations Publication. Sales No.: E.99.V.4, ibid., 24.

[171] See in this respect https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce and ibid., 21. The same aim of technology neutrality was employed in the(1999). Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions, Principles and guidelines for the Community's audiovisual policy in the digital age COM (1999) 0657 final. Brussels, Commission of the European Communities., whereby it is stated that there is as «a need for technological neutrality in regulation: identical services should in principle be regulated in the same way, regardless of their means of transmission». In a similar vein, the OECD stressed the importance of technology neutrality as a principle for Internet policy-making by stating that «maintaining technology neutrality and appropriate quality for all Internet services is also important to ensure an open and dynamic Internet environment» and «suppliers should have the ability to supply services over the Internet on a cross-border and technologically neutral basis in a manner that promotes interoperability of services and technologies, where appropriate». See in this respect OECD (2011). Council Recommendation on Principles for Internet Policy Making

[172] Greenberg, B. A. (2016). "Rethinking Technology Neutrality." Minnesota Law Review 100:1495., 1513. Also see(1999). Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, Towards a new Framework for Electronic Communications Infrastructure and Associated Services: the 1999 Communications Review COM (1999) 539 final, 10 November 1999 Brussels, Commission of the European Communities., 14: «Technological neutrality means that legislation should define the objectives to be achieved and should neither impose, nor discriminate in favour of, the use of a particular type of technology to achieve those objectives».

[173] Recital 18 of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) in OJ L 108 , 24/04/2002, 0033 – 0050. Similarly, Recital 34 of the Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services OJ L 337, 18.12.2009, 37–69, provides that «flexibility in spectrum management and access to spectrum should be increased through technology and service neutral authorisations to allow spectrum users to choose the best technologies and services to apply in frequency bands declared available for electronic communications services in the relevant national frequency allocation plans in accordance with Community law (the 'principles of technology and service neutrality')».

[174] Koops, B.-J. (2006). Should ICT Regulation Be Technology-Neutral?. Starting Points for Ict Regulation. Deconstructing Prevalent Policy One-Liners. It & Law Series, Bert-Jaap Koops, Miriam Lips, Corien Prins & Maurice Schellekens, eds. The Hague, T.M.C. Asser Press. 9: 77-108., 9, available at SSRN: https://ssrn.com/abstract=918746

[175] Greenberg, B. A. (2016). "Rethinking Technology Neutrality." Minnesota Law Review 100:1495., 1512-1513.

production»[176]. However, an empirical assessment – as the one performed by the Commission[177] – demonstrates how the same identical rules were not equally applied across all different kinds of products falling under its definition.

Undeniable differences emerge with respect to potential claimants, and defendants, as well as the respective economic power, and informational asymmetries. The greater or lesser relevance of the economic interests at stake also certainly plays a fundamental role.

Since the highest number of cases litigated involves raw materials, it is likely that those claims were brought primarily by one enterprise or professional against another one, not by a consumer. Moreover, technological complexity, in said cases, will certainly be more limited, and correspondingly the difficulty in identifying a causal nexus between the event and harm.

Pharmaceutical litigation, instead – the second most relevant domain per number of cases decided – [178], certainly involves both relevant economic interests and fundamental rights – people lives, health and physical integrity –, providing strong incentives for – even costly and complex – litigation.

Consequently, it is therefore not surprising – also considering limitations in compensable damages and the difficulty in meeting the burden of proof with respect to the notion of defect and causal nexus – that very few cases involved consumer goods of every-day use, and much less technological devices. In those cases, the defective nature of the product might have caused damages (i) of limited amount, and/or (ii) to interests that are not covered by the directive, including (iii) those to the device itself.

**Example 1**

> The malfunctioning of an external storage device (such as a hard-drive) due to a – manufacturing or design – defect, might have caused loss of data, that might not be compensable within the current formulation of the PLD[179]. At the same time, its overheating might have led to damages to other components connected to it – the personal computer for instance – that might be of limited economic value, thence either falling below the 500 euro threshold set by the directive, or anyway small enough not to justify suing the manufacturer on the grounds of the PLD, ascertaining the existence of a defect – in the design of the device or in its manufacturing – and of a causal nexus. Finally, the value of the hard drive itself might exceed that of all other damages suffered, and the user might seek redress within the limits of the CSGD, so long as the purchase could fall within that category – namely the parties being one a professional and the other a consumer – and the statute of limitations had not expired. In that case, however, he would not obtain compensation for the damage suffered, rather would either receive a replacement and/or reparation of the original device, or the reimbursement of – part or of the entire – resale price[180]. In any case, that would put the consumer in the same position as if the sales contract were correctly performed, namely ensuring the utility he originally pursued by acquiring the intended good. The PLD, instead, should make the claimant whole of the harm suffered, in the case at hand the further damages to the rest of the equipment, that would instead most likely not be compensated.

[176] 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, Official Journal L 210 , 07/08/1985, 0029 – 0033.

[177] Ernst&Young, Technopolis and VVA (2018). Evaluation of Council Directive 85/374/EEC on the approximation of laws, regulations and administrative provisions of the Member States concerning liability for defective products. Brussels, European Commission., 20.

[178] Ibid., 20.

[179] Expert Group on Liability and New Technologies - New Technology Formation (2019). Report on Liability for Artificial Intelligence and other emerging digital technologies., 59.

[180] See in this respect art. 3 (2) CSGD.

It could be argued that it is indeed a small claim, one of the kind the PLD did not intend to address, thence the 500-euro threshold. However, on the one hand similar kind of damages are precisely the consequence of «modern technological production»[181] the PLD intends to ensure compensation of or, said in economics terms, those externalities that enterprises selling products for profit should internalize. On the other hand, the aggregate value of said claims might be relevant, leading to inefficiencies and possibly also altering competition among enterprises. Indeed, those businesses that caused frequent little damages through the defective functioning of their products would successfully externalize costs, others have instead internalized, most likely at a greater cost and thence being disadvantaged on the market.

With increasing automation in daily life, many accidents won't be easily traced back to the direct intervention of a human being, even in those domains where today, instead, it is primarily if not exclusively so; moreover, new occasions of harm will potentially emerge as new services and opportunities that did not previously exist are offered, possibly leading to an expansion of the field of application of the PLD. If no human performs an action, or if a human collaborates with a machine in doing so, absent specific legal reform, the PLD will be applied, for damages that will result from the operation. Those damages will be – either solely or partially, according to whether a human being is involved in performance and might be blamed for the harmful occurrence – imputable to a malfunctioning in the device, thence, once more, a consequence of its design or construction.

Now, many of such claims will be of limited economic value to be compensated, or anyway to justify costly legal action, such as that the PLD presupposes (see Ch. 3, § 3.4.5 ), or again qualify as a damage – such as that to data – that does not appear clearly compensable.

**Example 2**

> The malfunctioning of a smart sensor inside a house regulating the air-conditioning system causes it to remain on at full power while the family is away for their summer holidays, causing an unusually high electricity bill due to the excess in energy consumption, and eventually leading to a relevant damage to the system itself.

**Example 3**

> the malfunctioning in a sensor causes an autonomous vehicle to collide with the one preceding it on the road. The accident causes a bump in both car's fenders, as well as some minor scratches.

In both cases, the overall amount of the damage might either be below the threshold of 500 euro, or above it, and yet insufficient to justify the ascertainment of a defect in the design or manufacturing of the sensors, as well as of a causal nexus between that and the damage suffered. Moreover, a part of the damage suffered by the owner of the apartment and of the vehicle causing the accident respectively, corresponds to the damaging of the smart air-conditioning system or of his own vehicle. Such damage, being referred to the defective good itself, would not be compensable pursuant to the PLD, thence a relevant part of the harm suffered due to the defective design or manufacturing would not be internalized. Both cases could find possible effective solution through first party insurance, but in any case that would not lead to the correct internalization of costs, possibly distorting competition as already clarified.

Such claims might appear trivial, and yet might be the most frequent kind. In particular, when products are conceived respecting high standards of *ex ante* safety investments, such as those that effective and stringent product safety regulation could ensure (see Ch. 3, § 3.1 above), the risk of relevant if not

[181] As stated in the recitals of the PLD, «liability without fault on the part of the producer is 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».

disastrous outcomes, leading to large economic losses, is going to be contained. The compound value of small inefficiencies, and defects leading to many limited damages might instead not be negligible.

To conclude, the underlying rationale of the PLD – which we have demonstrated is largely not achieved by the implementation of the directive (see Ch. 3, § 3.4 above), as it is also acknowledged by the proposals for reform advanced by the EG itself[182] – of ensuring compensation for damages arising from the use of products that are defective in that they lack the safety one would be entitled to expect in the given circumstances, is not intended to operate on a frequent basis, and for claims of limited value. When the directive was conceived, advanced technologies that either replaced human beings, or assisted them with relevant roles in the performance of complex tasks and in the delivery of sophisticated services reasonably were not anticipated by the legislator. Therefore, the PLD was intended as a rule to be applied less frequently than traditional tort and contract law, that would instead govern most accidents and harmful occurrences.

To the contrary, increasing automation inevitably causes a shift towards product liability rules in many domains that, previously, would only seldom, if at all, see its application[183].

Therefore, while it is certainly advisable to seek a revision of the PLD along the identified lines (see Ch. 3, § 3.5 above), the most suitable solution for losses involving the use of advanced technologies might be better pursued otherwise, through the adoption of ad-hoc legislation in those fields where it appears most necessary.

Indeed, a one-fits-all solution cannot be envisioned[184], for specificities become of relevance that may not be overlooked, and that entail both technological aspects and other inevitably connected ones, such as the nature of the product regulated[185], the size of its market, and that of a potentially connected insurance market, the kind and frequency, as well as the economic relevance of potential claims, and the qualification – as consumers or professionals – of the claimants themselves. Such a functional approach to regulation – that is at the basis of a RMA, defined below, (see Ch. 5, §§ 5.1-5.3) – to some extent defies «technological neutrality» but only if that is intended as a dogma. The PLD as it is today, in fact, despite being conceived as technology neutral, and thence applicable to any product, is actually not so, for only certain kind of litigations – with sophisticated parties involved, and/or relevant fundamental interests affected, and/or large economic claims – are carried out, as the clustering of cases primarily in a limited number of domains – as it emerges from the study conducted upon request by the EC itself[186] – confirms it.

Future proof regulation – that needs to be elastic – does not necessarily have to equate applications that are so diverse as those falling under the very notion of AI, and advanced technologies, that is by itself extremely broad, and destined to rapidly evolve over time with technical advancement (see Ch. 1, § 1.5). Therefore, the solution to the liability issues they give rise to may not be – solely or primarily –

[182] Expert Group on Liability and New Technologies - New Technology Formation (2019). Report on Liability for Artificial Intelligence and other emerging digital technologies., 27-28 and 42-43.

[183] Bertolini, A. (2016). "Insurance and Risk Management for Robotic Devices: Identifying the Problems." Global Jurist(2): 1-24.

[184] Bertolini, A. and E. Palmerini (2014). Regulating Robotics: a Challenge for Europe. Upcoming Issues of EU Law, available at http://europarl.europa.eu/document/activities/cont/201409/20140924ATT89662/20140924ATT89662EN.pdf. D.-G. f. I. Policies. Bruxelles.

[185] A device that promotes some fundamental values and rights of the individual, such as advanced robotic prostheses and exoskeletons do for people with disabilities, could deserve a particularly favourable liability system, easing its diffusion and adoption by a larger share of individuals, while the current could seriously penalize their diffusion. For a detailed analysis, in light of art. 4 let. G of the (2006). Convention on the Rights of Persons with Disabilities and its Optional Protocol (A/RES/61/106). U. Nations. which was adopted on 13 December 2006, ratified by the European Union on 21 January 2011, available at https://www.un.org/development/desa/disabilities/convention-on-the-rights-of-persons-with-disabilities.html, (last accessed, June 29th 2020), see Bertolini, A. (2015). "Robotic prostheses as products enhancing the rights of people with disabilities. Reconsidering the structure of liability rules." International Review of Law, Computers & Technology 29(2-3): 116-136.

[186] Ernst&Young, Technopolis and VVA (2018). Evaluation of Council Directive 85/374/EEC on the approximation of laws, regulations and administrative provisions of the Member States concerning liability for defective products. Brussels, European Commission., 20

achieved through the revision of the PLD, that is structurally extremely general in its application and incapable of accounting for those differences that yet persist.

Moreover, AI is pervasive. Its application will penetrate almost if not all domains of human applications, devices and services offered. Regulating AI will soon, and to some extent already today, entail addressing specific issues posed by AI in the most diverse domains, ranging from capital markets regulation, consumer services and products, transportation, medical malpractice, profiling, identification, competition law, and possibly discriminatory practices, to name a few examples. As those domains are addressed in very distinct fashions and with diverse approaches by legislators at both the European and MS level, so should liability aspects posed by AI applications in those very domains.

## 4.4. Seeking legal innovation: advancing user's protection beyond the «functional equivalent» argument

A relevant claim by the EG, is that «using the assistance of a self-learning and autonomous machine should not be treated differently from employing a human auxiliary»[187], similarly «[…] damage caused by defective digital content should trigger the producer's liability because digital content fulfil many of the functions tangible movable items used to fulfil when the PLD was drafted and passed […]»[188].

Those statements are, indeed, mere applications of the «principle of functional equivalence», whereby each person who suffers harm caused by AI-systems should have the same level of protection compared to cases without involvement of an AI-system.

The principle is unquestionable, and *per se* justifies interventions to improve the condition of potential victims of AI-based applications, in all those fields where a different outcome could otherwise be observed, less favourable than that which could be expected by the victim of non-advanced technologies. The EG addresses some of those concerns in its detailed analysis, thence reference to those considerations shall suffice.

However, the perspective of the policy maker intending to regulate emerging technologies could be more ambitious, actively seeking legal innovation that would improve the position of the claimant even further, while certainly not discouraging innovation.

Said otherwise, if the emergence of new technologies allows us to identify already existing weaknesses within the legal system – including, as pointed out by the EG, a relevant fragmentation among MS with respect to procedural rules, that have a significant bearing when attempting to establish the existence of a causal nexus, and fault when relevant[189] – that are not exclusively a matter of concern for emerging technologies – as it is indeed witnessed by the numerous attempts by national courts to overcome similar concerns in other fields through a number of doctrines, and theories of *prima facie* evidence, *res ipsa loquitur*, or «lowering the standard of proof in certain categories of cases»[190] – envisioned solutions should try to exceed the level of protection, and the overall efficiency achieved by the legal system so far, in non-technological fields. Indeed, when designing a new system, engineers always aim at exceeding the performance and efficiency of available alternatives; similarly, that should be the aim of the legal system to improve users' and third parties' protection further.

[187] Expert Group on Liability and New Technologies - New Technology Formation (2019). Report on Liability for Artificial Intelligence and other emerging digital technologies., 25.

[188] Ibid., 43.

[189] Ibid., 49-54.

[190] Ibid., 50.

After all, specialised areas of law – such as the emerging field of law and technology here considered – might represent a precious occasion to elaborate novel solutions to old legal problems, and said solutions, once tested through application, could then provide useful indications on how to reform general principles of law alike[191].

In such a perspective, if the current general principle for civil liability in all MS is fault based, the need to more frequently resort to strict liability solutions – if not absolute (see § 4.7 below) at times – in the case of technologically advanced products might suggest an overall reconsideration of the utility of fault in other regulatory fields. Indeed, already today some jurisdictions have adopted alternative mechanisms that heavily rely on automatic compensation, and no-fault schemes[192] in domains were most, yet not all MS[193], instead resort to traditional liability rules.

Implications are not of mere theoretical relevance, but might suggest the adoption of specific solutions that, for instance, depart from a rationale of blame and reprehension – typical of fault-based systems – , as well as from the need to clearly assess the existence of a causal nexus, pinpointing the «responsible party», to adopt a RMA, and one-stop-shop solutions, privileging the need to ensure compensation to the victim (see § 4.7 below).

Similarly, if some of the major concerns arise with respect to some substantial elements – such as the causal nexus, fault, defectiveness, and duties of care – the traditional solution elaborated by courts of reversing the burden of proof through a number of doctrines and theories elaborated on purpose, could suggest seeking alternative approaches, primarily grounded on different substantial norms, rather than procedural ones (more below § 4.6).

## 4.5. An overview of the alternative approaches proposed at European Level

There are a number of potential approaches to the adaptation of the legal system to the emergence of advanced technologies such as AI-based ones. Providing an exhaustive account is impossible, in particular because often times – besides more theoretical discussion of the kind already proposed (see Ch. 1, § 1.3.1, and Ch. 2, § 2.2) – the debate addresses specific applications, typically those that are already diffused (e.g.: drones) or attracting greater social attention, despite not largely deployed (e.g.: increasingly autonomous solutions); less frequently those that, despite largely distributed, operate in more restricted and isolated settings, and are thence less likely to attract the interest of the general public (e.g.: advanced industrial robots, Ch. 5, § 5.4).

The following analysis will focus on discussion occurring at EU level, thence addressing the report by the EG (see § 4.6 below), as well as the possibility to adopt a single rule of civil liability for all AI-based applications. Indeed, a discussion currently carried out within the Committee on Legal Affairs of the EU Parliament might move along this direction. The preliminary nature of the text debated (as presented on April 27, 2020 during a public discussion) does not suggest a detailed analysis of its content, still subject to change, and yet allows for more general considerations. (see § 4.7 below). Finally, an alternative approach will be presented, namely the RMA (see Ch. 5, §§ 5.1-5.3 below) with some

[191] See Castronovo, C. (2006). "Diritto privato generale e diritti secondi la ripresa di un tema." Europa e diritto privato., who applied this reasoning to competition law, consumer law and labour law.

[192] See Anderson, J. M., P. Heaton and S. J. Carroll (2010). The U.S. Experience with No-Fault Automobile Insurance. A retrospective. Santa Monica (CA), Rand. Feldthusen, B. (2002). "Posturing, tinkering and reforming the law of negligence – a Canadian perspective." University of New South Wales Law Journal Forum 8(2).

[193] In France the Loi n° 85-677 du 5 juillet 1985 tendant à l'amélioration de la situation des victimes d'accidents de la circulation et à l'accélération des procédures d'indemnisation.

https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006068902&dateTexte=20100114 establishes a non-fault based compensation solution for car accidents. (last accessed June 29th 2020).

exemplifications of how it could be applied to relevant technologies, highlighting the different policy outcomes it could lead to.

## 4.6. The Expert Group's report

In its assessment of existing liability regimes in the wake of emerging digital technologies, the New Technologies Formation of the Expert Group ("EG") claimed that: (i) the existing liability framework provided by the non-harmonized contractual and non-contractual liability ensures basic protection against damages caused by new technologies; (ii) nevertheless, certain characteristics of said technologically advanced applications may make it difficult for the victim to claim for compensation, ultimately resulting in an unfair allocation of the costs derived by technological development.

Against this background, the report suggested a series of solutions, adjusting both national and EU regimes (i.e. the PLD).

Firstly, it claimed that the person who operates a permissible technology, that nevertheless carries an increased risk of harm to others (e.g. an autonomous car) should be held strictly liable for the damages caused by the operation. However, when determining who operates the technology, it should be considered whether the back-end operator, such as the service provider, actually holds a higher degree of control on the technology. The leading rationale is thus that of holding liable the person who uses or benefits from the technology, and is in control of it.

As far as the nature of the liability involved, the report suggests a two-tiered approach.

If the technology involved does not pose a serious risk of harm to other, the operator should be liable for breach of the duties to select, operate, monitor and maintain said technology. He would thus be burned by a fault-based liability. In any case, when the application in question displays a certain level of autonomy, operators should not be subject to a regime of liability which is less severe than that provided for damages caused by human auxiliaries.

On the contrary, if technology exposes third parties to an increase risk of harm, the EG advocates a strict liability regime, often combined with compulsory insurance, where operators would be liable for any damage caused thereof, and would be covered by ad-hoc insurance.

The aforementioned regimes, however, would still be complemented by product liability rules. Indeed, in both cases manufacturers of products or digital content incorporating emerging digital technology should be liable for damage caused by defects in their products, even where such defects derived from changes made after that they have been put into circulation, if said changes were made under the control of the producer himself.

The report devoted particular attention to the problems connected to the difficulties experiences by the victims in proving the constitutive elements of the claims. In their conclusions, the experts suggested that, where a particular technology increases the difficulties of proving the existence of an element of liability beyond what can be reasonably expected, victims should be entitled to facilitation of proof. Also in the view of easing the evidentiary assessment, the study advocates for the development of logging features in the devices architecture, and for reversing the burden of proof to the benefit of the victim, whenever the operator fails to log or provide reasonable access to logged data.

Under this approach, the destruction of the victim's data should be regarded as damage, compensable under specific conditions.

### 4.6.1. Some critical observations

The EG report constitutes an important assessment of the current *status quo*, and many of its consideration regarding the inadequacy of the existing legal framework, in particular the factors limiting the victim capacity to successful claim compensation under EU or national law, are to be shared.

However, some criticism might be drawn to specific points of the proposal, namely : (i) the lack of a definition of advanced technologies their proposal should apply to; (ii) the difficult distinction between high and low-risk activities; (iii) the heavy reliance on evidentiary rules, over substantive ones; (iv) the not clear articulation of the relationship between the PLD and other ad-hoc liability regimes to be adopted; (v) the radical exclusion of electronic personhood as a viable alternative.

### 4.6.2. The lack of a definition of advanced technologies

As per *sub* (i), the report generically refers to «Artificial Intelligence and other emerging technologies»[194], and equivalent expressions. That of defining AI, robotics, and advanced technologies is, indeed, a daunting task, because so many diverse applications might fall under such broad notions that are not sufficiently defined, not even in a pure technological perspective.

However, as it was shown above (see Ch. 1, §§ 1.3 and 1.5), when used for normative purposes, the notion of AI is problematic, as it lacks any selective capacity, leading to unworkable legal uncertainties, and a potentially limitless application of the rules considered.

Indeed, the notion of AI might be considered a moving target, itself changing with technological advancement in a way that what might be deemed one of its applications at a given moment in time, might not be any longer classified as such later on, due to the overall evolution that makes the given technology – once ground-breaking – to become standard, if not obsolete.

Moreover, AI is pervasive, its applications will affect the most diverse fields of our lives, and subsequently of potential regulation. AI applications already today and ever more in the future will see applications in fields such as capital markets, medical practice (both in diagnosing and treatment), industrial production, 3d printing, autonomous and smart contracting, mobility management and transportation systems and solutions (including but certainly not limited to autonomous vehicles), assistance to – and in some cases cure of – frail individuals (children, elderly, people with disabilities), identification, policing and security enforcement, legal enforcement and administration of justice, consumer and household devices, management of human interactions and exchanges – for multiple purposes – over the internet (including but not limited to platforms). The list is potentially infinite.

On the one hand, those technologies have often times little, if anything, in common. Most certainly the kind of concerns they give rise to, from a societal perspective, are most often as diverse. Similarly, elaborated solutions should account for those differences, while only for limited aspects might be aggregated.

Pursuing a technology neutral approach at all costs – as for instance in the case of the PLD – will cause that any adopted norm will only be applied to those cases and those applications for which, ultimately, the legal structure provided appears adequate, in light of the incentives provided. In all other cases, that theoretically ought to fall under its field of application, practitioners and courts will still have to attempt to find alternative interpretative solutions. In the case of the PLD, as it was already shown, the clustering of cases clearly demonstrates that despite very broad in scope, litigation primarily emerged

[194] Expert Group on Liability and New Technologies - New Technology Formation (2019). Report on Liability for Artificial Intelligence and other emerging digital technologies., 3.

only in very clearly identified domains, with more sophisticated claimants, greater economic losses, and often involving the infringement of fundamental rights.

The EG stresses that no «one-size-fits-all solution»[195] can be advanced, and yet all its considerations are not technology specific, nor criteria are identified that clearly allow us to distinguish in which cases one alternative ought to be implemented and not another, when national legislations will suffice, or instead a specific intervention is advisable.

However, absent a more specific clarification of either the technology – or better class-of-applications considered – (see § 4.7 below) or of the relevant criteria for the apportionment of specific *Fallgruppen*, the adequacy of the solutions proposed may not be discussed in details.

### 4.6.3. The distinction between low- and high-risk

Indeed, the report acknowledges the difference and heterogeneity of AI-based applications, and the different legal, social and economic issue they bring about. Accordingly, it suggests that such applications shall be categorized according to what it considers to be a fundamental dichotomy, namely, that between low- and high-risk activities, to justify the operator's strict liability in case «emerging digital technologies […] are operated in non-private environments and may typically cause significant harm»[196], due to the «interplay of [its] potential frequency and the severity»[197].

However, this distinction, and the legal regime associated to it, are not free from criticalities. Indeed, the notion of low- and high-level risk may seem intuitive and familiar to some MS' legal systems, that adopt liability rules specifically dedicated to dangerous things and activities[198]. Nevertheless, it is not self-standing, but begs for further clarification. Furthermore, if considered in all its implication, it would lead to unjustified and undesirable practical consequences, and shall thus be rejected.

Firstly, the definition of «significant harm», upon which the distinction between low- and high-level risk is based, is problematic because it does neither identify an amount that would cause the harm suffered to qualify as «severe», nor a given frequency to be relevant for the same purpose. In that it does not possess any selective power, but simply entails a circular definition that does not allow to distinguish what ought to be deemed significant and what not.

This definition reflects the so called Learned Hand formula[199], adopted in the United States in the field of product liability, and which yet does not really possess – even within that context – a true operative value, for it is incapable of determining *ex ante* the correct threshold of safety investment demanded upon the producer to escape liability in cases of design defect, ultimately leaving large *ex post* discretionary powers on the judge deciding the single case. For the same identical reasoning, such an insufficiently *ex ante* defined criterion cannot provide useful objective guidance for policy-making. Indeed, it equates to stating that when the policy maker believes a technology to be high-risk it will regulate it as such.

---

195 Ibid., 36.

196 See ibid., 39, EG's key finding n° 9.

197 Ibid., 40, fn. 105.

198 As exemplified by the EG in ibid., 21 - see Article 1064 of the Croatian Civil Obligations Act (dangerous things and activities); § 2925 of the Czech Civil Code (extraordinarily dangerous operation); § 1056 of the Estonian Law of Obligations Act (major source of danger); § 6:535 of the Hungarian Civil Code (extraordinarily dangerous activity); Article 2050 of the Italian Civil Code (dangerous activity); Article 2347 of Latvian Civil Law (activity associated with increased risk for other persons); § 432 of the Slovakian Civil Code (extremely dangerous operation); Article 149 ff of the Slovenian Obligations Code (dangerous objects or activities). The French liability for things (Article 1242 of the Civil Code) is another peculiar solution not limited to any specific object or risk.

199 Grossman, P. Z., R. W. Cearley and D. H. Cole (2016). "Uncertainty, insurance and the Learned Hand formula." Law, Probability and Risk 5(1): 1-18. Geistfeld, M. A. (2011). Principles of Products Liability. New York, Foundation Press. 115 ff. Foerste, U. and F. Graf von Westphalen (2012). Produkthaftungshandbuch. München, C.H. Beck.

Moreover, so defined, the criterion does not take into account a fundamental constraint of emerging technologies, frequently recalled by scholars and practitioners alike, and to address which the EC is also actively funding research primarily through H2020 research projects, namely the unavailability of data with respect to the risks brought about by said technologies, as well as the need to develop new approaches to risk assessment, for existing ones are often inadequate, when technologies are considered that may be easily modified. In the field of autonomous vehicles, for instance, the data available with respect to their performance is largely insufficient even to justify the fundamental claim that they are going to be safer than human drivers[200]. Unknown unknowns, or «black swans»[201] are then a primary source of concern with respect to applications that might modify their functioning over time or, even more simply, be adapted for different purposes (such it is the case for collaborative robots, see Ch. 5, § 5.4), and the issue of benchmarking in robotics and AI is one of great technical concern[202].

Finally, this distinction does not constitute an adequate basis for determining what kind of liability rule should govern a case, fault-based or strict, as the definition of a liability regime should not be influenced by the amount of damage[203] a given application may potentially cause. Indeed, a very large harm both frequent or not, will almost always provide economic incentives that are sufficient to undergo even more complex litigation, such as that which requires the demonstration of fault, or even the causal nexus and defectiveness of the device as it is today required by the PLD.

At the same time, a small damage claim will not be brought even when a strict liability rule is in place – as it was largely discussed with respect to the PLD (see Ch. 3, § 3.4.4, and § 4.3 above) – if demonstrating other elements of the claim appears too complex, including causation.

Altogether, it is not evident why small claims that are not so frequent ought not deserve adequate protection by the legal system. Deciding whether a fault-based or strict liability rule is preferable ought to be determined in light of entirely different factors, such as:

a) the need to simplify a potentially complex overlapping of different liability rules, thence easing the identification of the *ex ante prima facie* responsible party (e.g.: one-stop-shop approach, see § 4.7 below);
b) the need to favour access to justice in claims where otherwise there would be no adequate incentives to sue, leading to externalization of costs by manufacturers, designers, and/or operators of a given technology (see § 4.7 below), eventually distorting competition;
c) the characteristics of the technology, its social desirability grounding arguments to favour its emergence[204], its potential diffusion, and the size of its possible market[205];
d) considerations about the (in)adequacy of the incentive structure derived from the existing legal system for the different parties involved (see Ch. 5).

To conclude, even if it were possible to calculate *ex ante* the significant nature of harm – or more precisely, in light of the definition provided, the average amount of damages a given technology might cause –, which clearly is not, that would thence not be an acceptable criterion to decide between a fault and a strict rule of liability.

[200] Kalra, N. and S. M. Paddock (2016). Driving to Safety. How Many Miles of Driving Would It Take to Demonstrate Autonomous Vehicle Reliability? Rand. Transportation Research Part A: Policy and Practice, 2016, vol. 94, issue C, 182-193.

[201] See Taleb, N. N. (2007). The Black Swan, Random House

[202] See Bonsignorio, F., E. Messina and A. P. del Pobil (2014). "Fostering Progress in Performance Evaluation and Benchmarking of Robotic and Automation Systems." IEEE ROBOTICS & AUTOMATION MAGAZINE(3): 22. and the COVR project funded from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 779966 available at https://safearoundrobots.com/.

[203] Indeed, by multiplying harm – thence damage – by the probability of its occurrence, a euro value of the potential claims, in aggregate form, is obtained.

[204] See fn. 185 above.

[205] See Bertolini, A. (2016). "Insurance and Risk Management for Robotic Devices: Identifying the Problems." Global Jurist(2): 1-24.

If we then move on to consider the exemplification provided, that too appears problematic and largely criticisable, implicitly referring to multiple criteria that, when analytically considered, appear to be apodictic.

Indeed, the EG states that

> «[for] the time being, [the opportunity to cause significant harm] applies primarily to emerging digital technologies which move in public spaces, such as vehicles, drones, or the like. Smart home appliances will typically not be proper candidates for strict liability. It is in particular objects of a certain minimum weight, moved at a certain minimum speed, that are candidates for additional bases of strict liability, such as AI-driven delivery or cleaning robots, at least if they are operated in areas where others may be exposed to risk. Strict liability may not be appropriate for merely stationary robots (e.g. surgical or industrial robots) even if AI-driven, which are exclusively operated in a confined environment, with a narrow range of people exposed to risk, who in addition are protected by a different – including contractual – regime […]»[206].

The criteria here identified are both technological and legal. Technological, in as much as what is deemed to be relevant is (a) whether the device has a physical body (implicit), (b) whether it operates in the public space, (c) whether it moves autonomously; legal, since (d) the availability of other compensatory regimes is considered.

*Sub* (a), the exclusion of non-embedded AI applications is unjustified, ultimately replicating the distinction between products and services, including software, that exists as of today within the PLD[207]. Relevant harm might be caused by applications that operate on capital markets to trade stocks or derivatives, provide financial consulting services, that profile individuals for multiple purposes, allow and facilitate exchanges of goods, services, and information (e.g.: platforms), that help in diagnose illnesses through imaging or consultancy, such as expert systems (see §5.6). Such applications might cause severe harm, both pecuniary and not, eventually affecting individuals' fundamental rights.

*Sub* (b) the distinction between devices operating in private and public spaces appears also apodictic. Indeed, how severe a potential harm might be –in terms of both the size of the damage caused, and the nature of the right or legally relevant interest affected – is unrelated to whether the place where the event verifies is open to the public or not. A smart-home application (e.g.: sensor controlling climatization) might harm the bodily integrity of the occupants of the house as much as a «delivery or cleaning robot», and even more dangerous appear to be industrial robots (independently of whether they are fix or moving) that do operate in secluded environment. Indeed, it is true in a public environment people are exposed to risks they did not consider and choose attentively. However, the contrary is not always the same for private places: people accessing private places – invitees of different nature – might not be aware nor willingly have accepted the risks posed by technological applications present in the given place. The need for a different kind of protection – and potentially a more stringent liability rule, such as a strict one – is totally unrelated to the public – or not – nature of the place where harm takes place, much more should rest upon considerations about the potential legal relevance of the interest affected, on top of all other elements identified under the letters above.

*Sub* (c), the ability to move, eventually «at a certain minimum speed», is also insufficiently defined, as well as apodictically selected as a prominent criterion to distinguish between a drone, which should be subject to strict liability in its operation, and a surgical robot, which, instead, should not. Indeed, it is

[206] Expert Group on Liability and New Technologies - New Technology Formation (2019). Report on Liability for Artificial Intelligence and other emerging digital technologies., 40.

[207] The contradictory nature of the statement can be observed by referring to EG's key finding n° 13 in ibid., 6 and 42-43.

not clarified whether any moving capacity should have a bearing on the liability regime or simply the ability to be autonomous. Yet, then autonomy ought to be defined. A machine could move and be remotely controlled by a human operator, such as in the case of a drone, or supervised (a garbage collecting applications such as Dustbot, developed by Scuola Superiore Sant'Anna), or also be totally independent, such as industrial robot that has an arm that operates at a great speed, or even an AV (industrial robot moving within a factory). What kind of movement – and why – would justify a more stringent type of liability is not clear, and yet numerous other technical elements are instead forgone that typically increase the level of risk an application possesses[208], and that are instead heavily debated in the engineering literature (including different of control systems).

Altogether, the features under point (a) (b) and (c) appear inadequate normative criteria for addressing liability derived from the use of AI-based applications, and the technical or legal reason for their relevance are hard to recognize. Indeed, they heavily relate to a corporeal notion of advanced technologies that leaves to the margin non-embedded AI applications, which instead will play an ever greater role, ultimately replicating the very distinction the EG criticizes in the PLD between products and services[209]. Moreover, their possible intersection appears confusing. Would a movable industrial robot, operating within the restricted environment of a factory, justify the application of a more severe standard of liability – strict –, and what about a robotic arm – that also moves but in a different way – should that, per se, be excluded?

In a policy perspective, taking into account the incentives that would emerge from such a system, we could then ask whether the EU should truly favour the development of fix robots – by applying a lower standard of liability upon those that make use of them – over movable ones, smart home applications over drones and driverless cars[210], and the like.

The only criterion that leads to useful considerations in a policy perspective among those identified is the one *sub* (d) above, i.e. the pre-existence of other – we should add efficient and effective – compensatory schemes. Said otherwise, if already applicable legislation already ensures an adequate level of protection, then there is no need to adopt a different standard of liability for the sole reason that some advanced technology is being employed.

This consideration is certainly relevant, and reflects the bottom-up, CbC approach that has long been suggested as the most appropriate in regulating any aspect of advanced technology[211], and proves the need to overcome a dogmatic approach to technological neutrality.

Indeed, adequate solutions might only be elaborated taking specific classes of applications into account, identifying their functioning and technological peculiarities, determining applicable existing regulation and how it interact and interferes with those traits, assessing the incentives it provides, and

---

[208] See fn. 202 above, as well as Salvini, P. (2013). Taxonomy of Robotic Technologies. Robolaw Grant Agreement Number: 289092, D4.1. for an exemplification.

[209] See fn. 207 above.

[210] Indeed, the EG seems to assume that a strict standard of liability is more punitive for the party than a fault-based regime, thence we can assume that, according to EG's reasoning, imposing a strict standard of liability upon a subject carrying out a given activity and or developing a given application entails disincentivising the same activity or the marketing of the application itself. This study suggests, instead, that in some cases, a strict standard of liability allowing for greater *ex ante* certainty and transparency could ease the diffusion of a given technology, and its early adoption by a larger number of users (see §§ 4.1 and 4.2 below).

[211] Please allow reference to Bertolini, A. (2013). "Robots as Products: The Case for a Realistic Analysis of Robotic Applications and Liability Rules." Law Innovation and Technology 5(2): 214, Bertolini, A. and E. Palmerini (2014). Regulating Robotics: a Challenge for Europe. Upcoming Issues of EU Law, available at http://www.europarl.europa.eu/document/activities/cont/201409/20140924ATT89662/20140924ATT89662EN.pdf D.-G. f. I. Policies. Bruxelles, Palmerini, E., F. Azzarri, F. Battaglia, A. Bertolini, A. Carnevale, J. Carpaneto, F. Cavallo, A. Di Carlo, M. Cempini, M. Controzzi, B.-J. Koops, F. Lucivero, N. Mukerji, L. Nocco, A. Pirni, H. Shah, P. Salvini, M. Schellekens and K. Warwick (2014). Guidelines on Regulating Robotics. Robolaw Grant Agreement Number: 289092, D6.2, Leenes, R., E. Palmerini, B.-J. Koops, A. Bertolini, P. Salvini and F. Lucivero (2017). "Regulatory Challenges of Robotics: Some Guidelines for Addressing Legal and Ethical Issues." Law Innovation and Technology: 1-44.

possibly inferring also form empirical considerations the outcome it might lead to, and ultimately, when necessary, elaborate an alternative proposal.

As stated above (see § 4.6.2), the extremely broad scope of the technologies addressed by the EG, and the insufficient definition of the object of their analysis – also as a consequence of the broad policy question raised by the European Commission when appointing it[212] –, makes it impossible to apply this methodology in their considerations, reaching very broad and general results that, however, could only be agreed upon were they more analytically referred to a specific class of applications, in light of the more stringent kind of analysis that is deemed necessary. As is, the considerations made appear too general and criticisable, for the reasons described.

### 4.6.4. Greater reliance on evidentiary rules over substantial ones, and on MS' legislation, leading to fragmentation

The EG dedicates a large part of its analysis to considering the apportionment of burden of proof, and evidentiary rules and doctrines – often developed through judicial application –, as both part of the problem and potential solutions to liability issues posed by emerging technologies.

Indeed, the EG's key findings nn° 15, 22, 24, 25, 26, 27 are directly related to those aspects, and EG's key finding n° 20 (on logging by design) is also tightly connected to some of those.

The fundamental idea underpinning all such considerations is that «where a particular technology increases the difficulties of proving the existence of an element of liability beyond what can be reasonably expected, victims should be entitled to facilitation of proof»[213]. This is typically observed with respect to the causal nexus[214] as well as the subjective element of fault[215], when relevant.

The difficulty is primarily argued upon technological complexity, and opacity[216], that also cause it to be particularly difficult to determine what happened, and pinpoint the liability upon a specific party, above all when more subjects cooperate towards the providing of a service or good (producer, programmer, service provider, infrastructure manager and the like). Moreover, this is a reason of specific concern in the field of product liability (see Ch. 3, § 3.4 above)[217].

At the same time, it is observed, when a manufacturer and operator face a victim, the former possess a better understanding of the technology, and better tools to interpret its functioning that is the necessary presupposition to be able to establish the existence of a defect, and/or a causal nexus, and/or of fault of any of the parties potentially involved.

The EG also acknowledges that MS legal systems, and in particular case law, has elaborated doctrinal solutions to achieve the reversal of the burden of proof[218].

[212] According to the official indication of the EC, the EG shall «[p]rovide the Commission with expertise on the applicability of the Product Liability Directive to traditional products, new technologies and new societal challenges (Product Liability Directive formation) and assist the Commission in developing principles that can serve as guidelines for possible adaptations of applicable laws at EU and national level relating to new technologies (New Technologies formation)»: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3592&Lang=IT (last access June 29th 2020).

[213] Expert Group on Liability and New Technologies - New Technology Formation (2019). Report on Liability for Artificial Intelligence and other emerging digital technologies., 4.

[214] Ibid., 21-22 and 49-51.

[215] Ibid., 23-24 and 52-54.

[216] Ibid., 32-33.

[217] Ibid., 42-43.

[218] Ibid., 50.

Most of these considerations are agreeable upon, and yet still give rise to some potential criticism, both with respect to the specific measures proposed, and more broadly, the perspective adopted, which favours procedural rules over substantial ones.

Under EG's key finding n° 15, dealing with producer's liability, it is stated: «if it is proven that an emerging digital technology has caused harm, the burden of proving defect should be reversed if there are disproportionate difficulties of costs pertaining to establishing the relevant level of safety or proving that this level of safety has not been met […]».

Since one of the most complex aspects of PLD litigation is that of establishing defectiveness as a deviation from «the safety which a person is entitled to expect, taking all circumstances into account» (art. 6 PLD), the reversal of the burden of proof with respect to the element of defectiveness – which pursuant to art. 4 PLD is to be demonstrated by the claimant – certainly entails a facilitation for the victim.

However, the reversal of the burden so conceived presupposes that the victim has already demonstrated causation, thence that it is the device that with its functioning led to the harmful event, and this is, by far, the most difficult element to ascertain, in particular given increasing complexity and interdependence of multiple factors in the causation of harm. Moreover, the reversal is made dependent upon «disproportionate difficulties or costs» that are not narrowly defined, and if so formulated in the legislation adopted, would certainly leave substantial room for uncertainty and discrepancies in its everyday application.

The need to alleviate the burden of proof with respect to causation is indeed addressed at EG's key findings nn° 25-26, whereby it is affirmed that, while this element should in principle still be demonstrated by the claimant (EG's key finding n°25), it

> «[…] may be alleviated […] if a balancing of the following factors warrants doing so: (a) the likelihood that the technology at least contributed to the harm; (b) the likelihood that the harm was caused either by the technology or by some other cause within the same sphere; (c) the risk of a known defect within the technology, even though its actual causal impact is not self-evident; (d) the degree of ex-post traceability and intelligibility of processes within the technology that may have contributed to the cause (informational asymmetry); (e) the degree of ex-post accessibility and comprehensibility of data collected and generated by the technology; (f) the kind and degree of harm potentially and actually caused» (EG's key finding n°26)[219].

Leaving aside detailed considerations about the single criteria proposed (lett. a through f), it shall be noted that the EG only formulates these considerations with the aim to «offer guidance on the further development and approximation of laws, and in order to allow for a more coherent and comparable line of reasoning» among MS, thence ultimately not «promoting any specific measure [that would otherwise] run the risk of interfering with national rules of procedure».

Said otherwise, the most relevant and complex element to be demonstrated in any litigation involving the use of advanced technologies would be left untouched, and only very general indication to alleviate the burden of proof ought to be formulated, to suggest MS and their court system to evolve into a given direction.

Such a conclusion appears largely inadequate to the task of improving the position of the claimant, and if at all heard by national legislators and judges called upon to decide in the single case, would still lead to substantial fragmentation in a very delicate aspect of the liability system, preventing any real

[219] Ibid., 49-50.

effort of harmonization, and ultimately leading to the creation of legal and technological barriers to the common market (Ch. 3 § 3.6).

Moreover, the consideration whereby leaving the burden upon the claimant, as a matter of principle (EG's key finding n°25) is an issue of fairness[220] is a quite debatable conclusion, that clearly depends upon an idea of civil liability as a form of individual reprimand.

Indeed, leaving the economic consequences of a harmful event on a victim is almost never fair. If it happens, in cases of complex and costly litigation such as those involving the use of opaque technologies – as so the EG defines them – it is most likely unfair for the victim and inefficient for a system that does not force upon those that derive a profit the internalization of the social costs they generate[221], as well as potentially a source of distortion in competitive markets (§ 4.3).

A different approach such as the RMA, adopts different kinds of considerations and more largely resorts to uniform substantive norms to ease the harmonization among MS in such relevant aspects of liability claims.

A similar reasoning to that underpinning EG's key findings nn° 25 and 26, grounds EG's key finding n° 27 that recites

> «If it is proven that an emerging digital technology caused harm, and liability therefore is conditional upon a person's intent or negligence, the burden of proving fault should be reversed if disproportionate difficulties and costs of establishing the relevant standard of care and providing their violation justify it […]»[222].

The corresponding analysis is accurate, and yet instead of suggesting the adoption of strict liability rules, whenever it is evident that fault would represent too serious a burden for the claimant, it is suggest to merely reverse the burden of proof without, however, specifying whether this should be enacted through a specific European rule, or whether the choice of its implementation should be demanded to the free choice of MS[223].

### 4.6.5. Logging by design

The opacity of advanced technologies poses the issue of the exact identification of the possible dynamics of the accident, in particular when multiple agents and factors are capable of influencing it.

As a consequence, the EG identifies as a priority the possibility to trace the different factors – eventually the autonomous decisions of the machine – so as to pinpoint the causal nexus, and determine one or more responsible parties.

In such a perspective EG's key findings nn° 20-24, affirm a principle of «logging by design» as a requirement that should be demanded of designers when appropriate and proportionate. More specifically, EG's key finding n° 22 establishes that «the absence of logged information or failure to give the victim reasonable access to the information should trigger a rebuttable presumption that the condition of liability to be proven by the missing information is fulfilled».

Therefore, failing to provide the recorded data – or failure of recording it in the very first place – might produce a reversal in the burden of proof in favour of the claimant.

---

[220] Ibid., 50.

[221] Think, for instance, in case of a bodily injury the costs associated with the cure and eventually permanent care of the affected individual that could burden the public healthcare and social security system.

[222] Expert Group on Liability and New Technologies - New Technology Formation (2019). Report on Liability for Artificial Intelligence and other emerging digital technologies., 52.

[223] Ibid., 55.

However, it shall be observed, it is sufficient for the defendant to concede access to the logged data, to avoid the presumption put forth by EG's key finding n°22. Said otherwise, so long as the designer or operator allows access to the information, nothing more is expected on his part.

Nonetheless, the most problematic aspect of said logged data is certainly its interpretation and analysis that might be extremely complicated and costly. Moreover, even the most accurate ascertainment of the dynamics of the event might be insufficient to establish liability.

**Example 4**

> A robotic hand prostheses, equipped with a logging device, is implanted onto an amputee. The human-machine interface that interprets the biological signal and transforms it in commands for the rotors allowing movement might, in some cases, misinterprets the signal and lead to an erroneous gesture or grip. If the amputee was allowed to drive a car – eventually adapted to his needs –, and were involved in a car crash where he got injured or died, or harmed third parties, he himself, his heirs, or the other victims might want to seek compensation. The amputee could be responsible of the accident – having maintained a negligent conduct – or, instead, the producer. In the latter case, the claimant would have to demonstrate that the human-machine interface misinterpreted the biological signal, causing an erratic, yet unintended hand-movement, which ultimately led to the crash, and all of this could be deemed the purport of a defect in design or manufacturing.

In such a case, logging could be problematic. However, if the manufacturer only ensured access to the data – most likely a very large amount of data – the claimant would still need to identify all the biological signals emitted by the nervous system of the implantee, identify those that might have been misinterpreted, demonstrate that if they were correctly interpreted there would have been no erratic movement on the side of the amputee, and without that movement the accident would not have occurred. Moreover, he would then need to demonstrate that the misinterpretation is a consequence of a defect existing at the moment the device was implanted.

Elaborating the amount of data in the first place, isolating the relevant portion, interpreting it, appears a daunting task and would still not satisfy the entire burden of proof the victim would have to meet. The fact that data is logged and eventually made available to the claimant *per se* does not appear to be sufficient. To the contrary, it could simplify the position of the producer or operator who could give access to an immense amount of information, leaving the counterparty the task of identifying the relevant portion (if it exists) and providing an interpretation of it. Such an operation would most likely be costly and unjustified with respect to the overall value of the claim in many cases – e.g.: a minor car crash with only material damages to the vehicles caused by the malfunctioning of a sensor in one of the two vehicles – that could however be frequent, and economically relevant if considered in aggregate value. This as well would prevent an effective internalization of costs by those that might give rise to risks – producers and operators – through certain applications, and leave the losses on innocent victims as well as owners (of a vehicle) in a perspective which also appears not to be fair.

A duty so conceived could instead be easily met and satisfied by the manufacturer or operator. At the same time, given the structural and unavoidable knowledge asymmetry it is also very likely that were the claimant capable of grounding a *prima facie* case of liability of the defendant, the latter could still identify other bits of information or provide alternative interpretations – in light of and thanks to his specific technical knowledge of the device he conceived, or operated – to rebut said presumption or piece of evidence.

A mere rebuttable presumption in case access to logged data is denied is thus largely insufficient to grant any effective protection to the victim.

### 4.6.6. Safety rules

EG's key finding n°24 deals with safety rules, stating that

> «where the damage is of a kind that safety rules were meant to avoid, failure to comply with such safety rules, including rules on cybersecurity, should lead to the reversal of the burden of proving (a) causation, and/or (b) fault, and/or (c) the existence of a defect».

Then comments that «failure to comply with rules» put forth by «the lawmaker, such as those adopted under the «New Regulatory Approach» and not mere standards developing in practice» should «lead to a reversal of the burden of proof concerning key elements of liability»[224].

This statement appears problematic.

We have already clarified the nature and relevance of product safety regulation (see Ch. 3, § 3.1 above) and we will further stress its importance in ensuring high standards of *ex ante* safety investments beyond that what could be achieved through liability rules (see Ch. 5, § 5.2 below). However, as of today, compliance even with harmonized technical standards – such as those recalled by the EG in its statement – is voluntary, and merely offers a presumption of conformity to product safety regulation, which is necessary to lawfully distribute a product on the market, and yet *per se* does not shield the producer from *ex post* liability claims.

Should the recommendation of the EG be implemented, manufacturers would have to conform to harmonized standards in order to avoid the reversal of the burden of proof. If, instead, they complied with product safety regulation otherwise, as they are authorized to do today, and not by resorting to harmonized standards – which anyway account for a minimal portion of all the existing and commonly applied technical standards at European and international level –, a claimant could more easily trigger the reversal of the burden of proof, despite not having demonstrated that the application was indeed dangerous, or lacking the safety expected, as required by the PLD.

At the same time, demonstrating the violation of harmonized standards is most likely neither easy nor cheap on the side of the victim, requiring complex technical ascertainment, that would only be proportionate in the case of economically relevant claims, allowing for the same critical considerations drawn above (see § 4.6.5 above).

### 4.6.7. The relationship between producer's and operator's liability

The EG addresses relevant criticism to the PLD and proposes modifications[225] that might largely be shared, including overcoming the development risk defence (EG's key finding n°14), as well as the need to eliminate a rigid distinction between products and services that might not account for all contemporary business models[226] – despite the considerations drawn above (see § 4.3) –, while evidentiary aspects have already been discussed (see § 4.6.4 above).

At the same time, the operator's strict liability is proposed that – despite the critical observations formulated above with respect to the categories of applications it should apply to (see § 4.6.3 above) – might as well prove a desirable alternative, in selected cases to be better specified.

How these two forms of liability coexist and interact is, however, not clarified. The proposed criteria for cases of multiple tortfeasors (EG's key finding n°31) could apply, despite the provided examples deal with alternative causation scenarios. The proposal to allow for joint and several liability, and incentivise

[224] Ibid., 49.

[225] Ibid., 42-43.

[226] Ibid., 43.

legal arrangements on the apportionment of liability between parties that collaborate towards providing a given product of service[227] should also be commended as particularly useful.

### 4.6.8. The legal personality of the machine

The present study has already clarified why a radical rejection of the possibility of attributing the machine legal personhood appears apodictic (see Ch. 2, §§ 2.2-2.3 above).

Here we shall only further stress the example provided by the EG – that of a driverless car – is certainly inappropriate, and yet not the only possible.

**Example 5**

> A non-embedded AI expert system is deployed to deliver consultancy and data analysis over the internet, as a service to multiple users. The code might be modified by entities that provide training services, upon a client's request, to adapt the system to his needs, and the algorithm also modifies itself over time, through its operation.

Multiple parties could be potentially liable in such a scenario. Attributing legal personhood to the machine, eventually demanding its registration and compliance with public disclosure duties to be defined, requiring a minimal capital, and eventually the subscription of insurance coverage, could allow the system to become the entry point for all litigation (equivalent to a one-stop-shop solution). Those that contribute to its creation and operation could possess shares of the legal entity, being entitled to subsequent cash flows generated, and also bearing the economic consequences of liability in proportion. At the same time, the operation of the system could provide revenues that would integrate its assets to be then used to meet all sorts of obligations (arising from liability, thence compensatory, as well as contractual relationships and legal obligations).

Establishing a corporation to operate the AI-solution described in Example 5 above could lead to equivalent results, but regulation of an electronic person as opposed to a corporation might differ on a number of grounds, including alternative – both more or less favourable – tax regimes, as well as capital and insurance requirements, organizational structure, registration and disclosure duties.

### 4.6.9. Some overall considerations

To conclude the overall assessment of the proposals formulated by the EG, reference can be made to the duties of care (EG's key findings nn° 16-17), insurance (EG's key finding n°33) and compensation funds (EG's key finding n°34).

With respect to the former, it is particularly sensible to extend manufacturers' and operators' duties to the postcontractual phase[228], to include monitoring, maintenance and update duties. Postcontractual obligations are not largely regulated at European level, and efforts may be made to elaborate them through case law, by referring to general clauses such as good faith[229]. Similar obligations are particularly relevant when emerging technologies are concerned, considering the need for their constant revision and adaptation through subsequent patches. In this sense, it is also sensible to burden the producer or operator with the duty to update – software and applications alike – to ensure

---

[227] Ibid., 58.

[228] Please allow reference to Bertolini, A. (2018). "Human-Robot Interaction and Deception." Osservatorio del diritto civile e commerciale, Rivista semestrale(2): 645-659.

[229] Such as in the case of the German *Ersatzteilbereithaltungspflicht*; for a discussion in this respect see Palmerini, E. and A. Bertolini (2016). Liability and Risk Management in Robotics. Digital Revolution: Challenges for Contract Law in Practice. R. Schulze and D. Staudenmayer. Baden-Baden, Nomos: 225-259.

compliance. This, for instance, becomes of essential relevance in cases such as autonomous vehicles, contradicting the approach as of today adopted by the German legislator.

Similarly, considerations about – compulsory – insurance can be agreed upon, in particular stressing the importance of cost internalization that said solutions ensure (see Ch. 5, § 5.2 below). However, it is also true that an insurance market for given products and services might not exist. This could depend upon the risks being too high, difficult to restrain and calculate (also see § 4.6.3, and the references there made to issues of risk assessment and benchmarking), or the limited number of users of a given technology in absolute terms or in proportion to the risks identified.

When market solutions fail, and thence insurance is not available, when relevant no-compensation funds could be put into place. The EG acknowledges their importance, but limited to the cases where compensation needs to be provided when an accident is caused by unidentified or uninsured tortfeasors.

The spectrum of useful applications of no-fault compensation funds – both publicly and privately managed – eventually funded through taxation, could instead be much broader in a RMA perspective and could prove a viable alternative to insurance mechanisms in cases of market failures[230] (see Ch. 5, § 5.3).

## 4.7. Adopting a general liability rule for civil liability arising from the use of AI-based system: critical remarks

The analysis of the EG while clearly admitting the impossibility of a one-size-fits-all solution[231], might be interpreted as suggesting a cross-cutting regulation of advanced technologies, absent a clear definition of the object being discussed, the broad categorization according to the awaited level of risk, and the wide array of examples considered in its discussion.

Indeed, as clarified above (see Ch. 1, § 1.5), defining AI unitarily is impossible, and yet clearly identifying the object being regulated is an unavoidable condition, for the scope of application of any norm needs to be precisely determined for minimal legal certainty to be achieved.

To address this fundamental concern, two alternative approaches might be adopted.

A first option is that of providing a general definition, with an extremely broad scope of application – such as the notion of product for the PLD –, would simplify the regulatory effort and allow the adoption of one single legal act to address multiple technologies.

A second option is that of proceeding on a technology-specific basis, identifying single classes of applications that need to be separately regulated with independent normative acts, narrow tailored to address existing concerns, and provide adequate incentives.

The second option appears preferable for the reasons already discussed, namely the profound and unavoidable differences among different uses of AI, the pervasive nature of such applications – being deployed in the most diverse fields of human activity –, ultimately causing different problems to arise that are specific for one class of applications, and not for others, therefore demanding as specific solutions. It is certainly more demanding on the side of policy-makers, requiring a greater effort, and yet appears to grant greater legal certainty, and adequate responses to the multiple parties involved

[230] See Anderson, J. M., P. Heaton and S. J. Carroll (2010). The U.S. Experience with No-Fault Automobile Insurance. A retrospective. Santa Monica (CA), Rand.; Cuocci, V. V. (2013). Dall'assicurazione obbligatoria R.C. Auto alla no-fault insurance. Uno studio comparativo dei sistemi di traffic accident compensation. Milano, Giuffrè.

[231] Expert Group on Liability and New Technologies - New Technology Formation (2019). Report on Liability for Artificial Intelligence and other emerging digital technologies., 36.

(researchers, producers, professional and final users). Moreover, it avoids unnecessary regulation – of those technologies that do not pose relevant concern –, and possible interferences with MS legislation that could be deemed not fully respectful of the principles of subsidiarity and proportionality.

Ultimately, the second option would also be coherent with the approach adopted as of today both at European and MS level, which has always been technology-specific. Indeed, drones, driverless cars, platforms have been so far regulated with separate normative acts, and doing otherwise would most likely led to too general and ineffective outcomes.

However, the following chapter is entirely dedicated to discussing the second option, by introducing in more detailed terms the so called Risk-Management Approach (see §§5.1-5.3) in its theoretical (see § 5.2) and methodological (see § 5.3) implications, to then consider specific domains where intervention by the European Union should be considered, despite with diverging conclusions.

In the following paragraphs (see §§ 4.7.1- 4.7.6 below), instead, the first option will be addressed, discussing the major concerns it could give rise to.

In both cases, it shall be noted, one element appears to be shared, namely the need to prefer solutions that hold the party liable that is in the best position to identify, control and manage a specific risk. This is but one of the defining elements of a RMA.

### 4.7.1. The problems in elaborating a uniform definition of «AI-based applications», and its effect on legal certainty.

The major concern when attempting to elaborate a single body of legislation for all advanced technologies is that of providing a sufficiently wide definition. As it was clarified above (Ch. 1, § 1.5) this would prove a daunting task, doomed to be at once over- and under-inclusive.

Indeed, it would have to refer to those criteria that are commonly recalled to discuss AI in general terms, typically autonomy, the ability to learn and self-modify over time. However, even those characteristics come in a broad spectrum, and might be achieved through different methodologies, leading to substantially different results. A self-learning tooth-brush, as well as a modern camera trigger could be deemed autonomous AI-based applications, falling under a broad notion of advanced technology, defined according to those elements. Yet, in most cases, those applications do not give rise to any societal concern, and do not deserve the attention of the European legislator. Other, and more novel, subsequently developed techniques might instead not be encompassed.

Moreover, uncertainty would result from such an effort even with respect to the distinction between the scope of application of such a European legislation and MS's internal rules of liability. The pervasive nature of AI will, in fact, soon cause autonomous and self-improving solutions to be deployed in the most diverse fields, most of which, as of today, are regulated at national level.

European law would, in such a perspective, automatically and often unintendedly, attract under its competence entire fields today regulated by MS legislation and general principles of contract and tort law, in a way that is neither appropriate and useful to avoid market and legal fragmentation, nor fully respectful of the principles of subsidiarity and proportionality.

Indeed, in many cases a European intervention is advisable, and in such cases, most commonly maximum harmonization should be pursued, yet those cases should be carefully analysed, and discussed, and such a conclusion reached taking into account the European relevance of the matter.

Finally, a uniform solution will most likely not be adequate in most cases. Indeed, many of the fields where AI is and will be deployed are separately regulated today, both at national and European level.

This is the case for, as a mere example, medical malpractice, the responsibility of custodians of things and animals, intermediaries' liability, and that of owners and drivers of vehicles. If liability norms adopted in those fields are as of today distinct, and abiding different criteria and principles, the fact that some AI-based solution will be used, does not represent sufficient an argument to address them unitarily, with a single norm or set of norms. Such an effort will be suboptimal in most circumstances.

### 4.7.2. Classifying applications, and the distinction between low- and high-risk

A way to address this concern is that of introducing internal classifications, to group and separately list different technologies. That, indeed, would limit uncertainty specifying the applications that fall under such a European legislation, determining which are governed by one principle or another. Certainty would be achieved so long as the list was precisely defined, and possibly closed, limiting the possibility of extensive interpretation, rather relying on constant update. In such a perspective, the EG proposes a classification according to the anticipated level of risk posed by single devices (see § 4.6.3 above).

However, in general terms any such classification is only good and useful so long as it is very narrowly defined and groups applications that are better addressed as such. The anticipated level of risk is therefore insufficient. To exemplify, should driverless cars and drones be perceived as determining an identical high-level of risk – both operating in public places and exposing potentially unidentified parties to harm – applying an identical liability rule, holding the same party liable, is most likely still not the preferable solution. If, in the first case, it might be sensible to burden the owner or producer (see § 5.5 below), in the other case the operator is most likely best positioned to ensure compensation (see § 5.7 below).

Ultimately, an adequate classification would require the same level of specificity suggested in the second option, pursuant to a RMA, as described below (see § 5.1), that would also be coherent with the approach adopted as of today both at European and MS level, thence regulating specific technological applications separately.

Finally, to justify the need for regulation, reference to the anticipated level of risk is both problematic and excessively limiting the freedom of the legislator. As per the first profile, we might refer to the considerations drawn with respect to the report of the EG. In particular, it is not possible to truly calculate the amount of potential risks – in terms of awaited damage and likelihood of its occurrence – with respect to single classes of applications. Not only is there a lack of statistically relevant data about novel devices, but assessment methodologies are also deemed inadequate (see § 4.6.3 above, and fn. 202). In any case, such evaluations might only be performed *ex post*, once risks materialize and they could only be of partial utility when grounding the decision of the policy-maker to intervene.

As per the second profile, policy makers might decide the need for a normative intervention based on a multiplicity of considerations that go very well beyond awaited risks, eventually relevant also to select a specific liability rule (strict, absolute or fault based) over another one. The nature of the rights being threatened (e.g.: privacy), the societal desirability of a technology (e.g.: robotics prostheses and exoskeletons), or the need to protect a specific category of individuals (e.g.: medical practitioners from excessive litigation, see § 5.6), to name a few examples, are all as valid criteria as the level of risk to induce policy-makers to conclude there is a need to intervene, and eventually through which kind of norm (strict, absolute or fault based). Selecting a single and universal parameter according to which all policy decisions should be justified, appears as an excessive self-limitation for European regulators.

### 4.7.3. Avoiding victims (under)compensation

Liability rules are typically thought of serving to purposes, *ex ante* deterrence and *ex post* compensation. *Ex ante* deterrence is achieved by threatening the rationale agent of forcing him to compensate the damage caused, so that anticipating the subsequent loss, he will adapt his conduct – the efforts and the investment he makes – to avoid causing harm in the first place.

*Ex post* compensation forces the responsible party to internalize the loss he caused, when it can be demonstrated he was responsible, making the victim whole.

Balancing these perspectives is also perceived as essential to ensure an equilibrium between the agent's freedom to act and the right of the victim not to be harmed. Indeed, not any conduct needs to be prevented, and not any risk. In the current setting, the interest of the producer/user/service provider adopting AI-based solutions to innovate needs to be balanced with that of the victim of being compensated.

However, the effectiveness of liability rules in optimally deterring the agent's undesired behaviour is highly questionable. Very often other mechanisms, such as reputation and market competition, are much more effective in inducing an adequate effort and *ex ante* investment on the side of the party that would then have to compensate damages (e.g.: the producer in the PLD)[232]. Moreover, product safety regulation (see § 3.1 above) are also more effective in identifying the effort demanded to professionals attempting to offer goods and services on the market for profit (§ 3.5).

Empirical studies have been conducted in specific fields – aviation – that appear to confirm this conclusion[233].

At the same time, burdening agents with liability to ensure victim compensation is not necessarily detrimental for innovation. Indeed, if victims increase their trust in technology because it is intrinsically safe – since high *ex-ante* standards of product-safety are required through technical regulation (see § 3.1 above) – and because they know they will achieve compensation – should they nonetheless be harmed – they will more easily purchase the technology.

A good example in this perspective is offered by the CSGD. The two-year legal warranty, whereby the consumer can easily obtain the replacement of a non-conforming good – or the restitution of the resale price – is highly valued, and many are induced to purchase the good on the European market over cheaper alternatives due to that clear and effective *ex post* protection. This certainly benefits the market, producers and resellers alike.

Legal certainty and effective legal protection increase users' trust and willingness to purchase more innovative goods.

Trust is achieved when victims are aware that they will always obtain compensation if they are entitled to it. A victim is entitled to be – at least partially – compensated whenever she is not exclusively responsible for the damage suffered.

However, in many cases a victim who is not responsible for her own harm might not be able to establish before a court the liability of any of the potential tortfeasors, and therefore will be left without compensation, even if, in principle, she would be entitled to receiving it.

[232] Posner, R. (2007). Economic Analysis of Law, Wolters Kluwer. 182, Polinsky, M. A. and S. Shavell (2009-2010). "The uneasy case for product liability." Harvard Law Review 123: 1437.

[233] Helland, E. A. and A. Tabarrok (2012). "Product Liability and Moral Hazard: Evidence from General Aviation." The Journal of Law and Economics 55: 593. For a discussion of this aspect in the framework of technology regulation, please allow reference to Bertolini, A. (2016). "Insurance and Risk Management for Robotic Devices: Identifying the Problems." Global Jurist(2): 1-24.

This occurs because of failures in the legal system, due to the cost of accessing to justice or the complexity of the legal framework, leading to the potential overlapping of liability rules and a multiplicity of potential tortfeasors. «Alternative causation» – whereby many parties might have contributed to causing harm and yet it is not obvious which one pre-eminently or exclusively caused it, and thence should be held responsible – is particularly problematic in this perspective, often causing victim undercompensation even in non-technologically advanced fields.

Such problems are also considered by the EG, who acknowledges that if «it is already difficult to prove that some conduct or activity was the cause of harm», «it gets even more complex if other alternative sources come into play», and that this scenario «will become much more of an issue in the future, given the interconnectedness of emerging digital technologies and their increased dependency on external input and data, making it increasingly doubtful whether the damage at stake was triggered by a single original cause or by the interplay or multiple (actual or potential) causes»[234]. Indeed, the EG clarifies, existing national tort laws resolve these cases so that «either 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». Thus, it is indeed possible that the claimant does not manage to get compensation.

Such cases are clear failures of the legal system, for it causes a discrepancy between reality – what happened: namely the victim was hurt, and someone must have caused such harm – and legal reality, which is what may be demonstrated in a court, before a judge.

One of the major issues with emerging technologies is that demonstrating responsibility might become ever more difficult due to (i) the opacity and complexity of the technology itself, and (ii) the overlapping of different liability regimes that do not allow to identify one clear entry point for litigation – one-stop-shop approach (see Ch. 5, § 5.2) –, and (iii) the complexity of evidentiary rules when applied to the technology due to *sub* (i) above.

Any policy initiative should address both (ii) and (iii) and refuse the idea that a victim who suffered harm and did not cause it herself, might be left without compensation. To achieve that at times – as we are here suggesting, and by analysing single scenarios of potential application of different classes of technological devices and services – legal reform and simplification is necessary. Very often – even if not always – identifying a single-entry point for all litigation – one-stop-shop approach – is the preferable alternative.

### 4.7.4. Identifying a single entry point of litigation

Identifying a clear, sole responsible party towards the victim is of primary importance to ensure compensation, for it would avoid the alternative causation scenarios described above.

This is a preferable solution even in cases where it would still be uncertain whether that one specific party is responsible for the harm suffered, or instead someone else contributed to it, so long as secondary litigation rights are granted, as well as contractual mechanisms favoured.

Indeed – as the EG itself suggests[235] – rights to sue in recourse along the value chain, and/or towards other potentially responsible parties – either for identified shares (several) or pro quota (several and joint liability) –[236] allows for a more effective distribution of the economic loss.

[234] Expert Group on Liability and New Technologies - New Technology Formation (2019). Report on Liability for Artificial Intelligence and other emerging digital technologies., 22.

[235] Ibid., 22. See also EG's key finding n° 23.

[236] Ibid., 57-58.

The outcome is fair: the victim who did not contribute to causing the harm is compensated. Those that benefitted economically – selling for profit the good or service –, and through price mechanisms those that benefitted of the use of the good or service – users – (see Ch. 5, § 5.2 below) pool and share the loss[237].

The outcome is efficient: it reduces the complexity and therefore costs of litigation. Ultimately it eases access to justice for all, and favours innovation: it increases trust in the use and reliability of technologically advanced solutions, favouring the early adoption of technology (see Ch. 5, §§ 5.1- 5.3 and § 5.5.3).

### 4.7.5. The need for a narrow-tailored definition of the responsible party

To clearly identify a single entry point of litigation it is essential to define it narrowly.

Indeed, if adopted legislation resorted to an umbrella-term[238], potentially encompassing different parties at once (e.g.: the producer, owner, professional and or private user, custodian, service provider), many subjects could be deemed responsible towards the victim, and determining which one to sue would again become costly, discouraging access to justice and leading to undercompensation in alternative causation scenarios described above.

This might also lead to overdeterrence, in particular when duties to insure are established upon the responsible party. Indeed, if more than one of the agents involved in the production, use or provision of a good or service were to qualify as potentially responsible parties, they would all need to insure against the same harm, leading to an increase in the cost of good or service, beyond what is reasonable and useful. This would also delay innovation.

**Example 6**

> A passer-by crossing the street on a zebra crossing is run over by a car with some degree of automation. The possible responsible parties are the car owner, the driver (who might not correspond to the owner), the internet service provider that connects the vehicle to the smart road, the infrastructure service provider, the producer, and, should the driver be using a mobility-as-a-service solution, even the company that provided that service. All these parties theoretically might fall under an identical umbrella term. The accident will either be due to a system error in the vehicle, the erroneous choice to use some autonomous function on the side of the user, a problem in the internet connection or in the smart road functioning. One or more parties could be responsible for that risk, and yet which risk exactly materialized is not obvious.

The victim could either choose one party and sue that one alone, risking that the judge finds that someone else is liable, among the others, or sue all of them increasing the cost of litigation. Eventually, those high costs could discourage him from suing in the first place, and would not see the damage compensated.

The need to resort to a very general definition – or umbrella term – to identify the responsible party is consequential of a choice to regulate all advanced technologies unitarily. Indeed, if an identical liability rules needs to apply to driverless cars, drones and expert systems – to mention a few examples – it may

[237] It shall be stressed, that also in cases of Acts of God, where no party might be deemed liable, it is still preferable to favour some form of socialization and distribution of loss, rather than leaving it entirely on the single party who won the negative lottery.

[238] This seems to be the case with the notion of «deployer», defined by art. 3 let. d of the Draft Report with recommendations to the Commission on a Civil liability regime for artificial intelligence (2020/2014(INL)) as «[…] the person who decides on the use of the AI-system, exercises control over the associated risk and benefits from its operation». See – Committee on Legal Affairs (2020). Draft Report with recommendations to the Commission on a Civil liability regime for artificial intelligence (2020/2014(INL)), European Parliament.

not be sufficiently specific not even with respect to the subject who is identified as primarily responsible.

To exemplify, if drones most commonly – even if not always – have an «operator» (see § 5.7), driverless vehicles typically do not, because they are privately owned, and used – for the most part, unless mobility as a service is considered – (see § 5.5 below); in a medical setting, instead, that could be understood as referring to the doctor or practitioner using the device, that would be an entirely different subject, in a completely different position (see § 5.6 below), and one that should be shielded of responsibility rather than burdened, as opposed to unmanned aircrafts.

Said otherwise, legislation that attempts to regulate technology unitarily or at least with a cross-category approach cannot avoid being generic in the identification of the responsible party, with the consequences described above.

Finally, instead, which party is best positioned to identify, control and manage a risk is very much specific for different classes of applications. For instance, in some cases, it may be appropriate to hold primary responsible the operator (e.g. drones); in others, the business user and/or system integrator (advanced industrial robots), the service provider or deployer (AI-based consultancy services), the hospital and/or medical structure, and/or service provider (in case of medical diagnosis), the producer and/or the owner (in increasingly autonomous vehicles; for an analysis of these different types of liability, see §§ 5.4-5.7 below)

Such an approach is both more efficient in ensuring adequate incentives to all the parties involved, favouring innovation, and is also more consistent with the one adopted so far at MS's and European level when regulating civil liability, not only with respect to technology.

### 4.7.6. Compensable damages

Damage capping is a useful and appropriate solution in particular when strict – or absolute liability – rules are put in place, in particular in a risk-management perspective, such as in the proposed regulation, whereby the party is held liable that is best positioned to identify the risk, control it, and manage it, also through insurance mechanisms.

Damage caps, however, should be commensurate to the risk posed by a given technology, for liability should maintain a compensatory nature.

In such a perspective, identifying a single liability cap applicable across categories of different technological applications would be practically difficult and, most importantly, may lead to undesirable results. For example, caps may turn out to be excessively disproportionate in respect to the harm suffered by the victim, leaving her substantially undercompensated, and thus deprived of judicial protection. Especially where fundamental rights are violated, liability caps may indeed be deemed unconstitutional.

As we clarified in §3.5, civil liability rules are primarily directed to compensate the victim, so that compensatory damages shall be awarded as to put the infringed person in the same position he would have been in, had the damage not occurred. In this sense, both national and EU liability rules envisage limited variation form the so called «compensatory principle»: for specific wrongs, statutes may introduce criteria for the quantification of the damage that lead to either a reduction – as in the case of caps, made to limit liability in case of harmful yet socially desirable activities – or an expansion of the award – as in the case of disgorgement damages, which aim at punishing the defendant by stripping him from the profits made through the infringement –. However, when a mismatch between the damage suffered and the award granted to the victims is allowed, this should not be such as to substantially deprive the victim of the compensations he deserves. In this sense, if the «compensatory principles» shall not be intended as a strict correspondence between the damage suffered and the remedy awarded to compensate for it – *«tout le dommage, rien que le dommage»* –, but rather as an expression of the principle of protection of fundamental rights, as well as the very principle of effective judicial protection – belonging to the constitutional tradition common to the MS and enshrined in EU Treaties and Charters –, which require that effective redress is granted[239].

More generally, they might be adequate only for some kinds of applications, also suggesting the adoption of a more granular approach, taking into account the nature of the harm threatened, the rights it infringes upon, as well as the numbers of potential victims.

The nature of the risks generated by a driverless car operating on a public road, are not comparable to those of a drone with a small mass used for recreational purposes, or an AI-based system used for financial trades on the stock-market.

Finally, it is not advisable that damages be limited by enumerating some categories and excluding others (e.g.: life and bodily integrity, but not other non-pecuniary losses). MS have adopted different approaches in this respect, and interfering with such principles could lead to potentially unconstitutional results[240].

### 4.7.7. Final considerations

The preceding paragraphs have discussed the possibility of regulating advanced technologies unitarily, highlighting the major concerns such an approach gives rise to (see §§ 4.3- 4.7).

Those could be summed up, saying that technological complexity cannot be reduced, and differences overlooked. Those inevitably reflect upon the choice of the optimal liability rule (see § 4.3 - §4.4).

Moreover, such an effort would require so broad a definition of technology that would most likely be both over- and under-inclusive, in any case leaving uncertainty with respect to the applications addressed. This, in turn, could also cause problems and unjustified interferences with MS's legal systems and their general responsibility rules (see §1.5 and § 4.7).

Technology regulation should optimally occur at EU level, and seek maximum harmonization, but only in those fields where it is strictly necessary, and in a way that is respectful of the principles of proportionality and subsidiarity. A general rule, applicable across categories, would most likely be more problematic in such a perspective ( see § 4.2 and § 4.7). This is also in line with the «better regulation» guidelines adopted by the European Commission on 7 July 2017 [241].

If classifications were introduced, distinguishing within applications, those to be effective would have to be so specific as to abide a CbC approach as that described under the RMA below ( § 5.1).

[239] For an account of the compensatory principle in European and MS tort law, see Koziol and Wilcox (2009). "Punitive Damages: Common Law and Civil Law Prospectives." Tort and Insurance Law 25 (Institute for European Tort Law of the Austrian Academy of Science). In Italian law, a revision of the so called «principio di riparazione integrale del danno» derived from the famous decision of the Corte di Cassazione, n. 16601, 5 luglio 2017, which recognized – in limited circumstances – the possibility for an Italian judge to recognize and enforce a foreign judgement awarding punitive damages under private international law rules.

[240] Indeed, the majority of MS do not enumerate the kind of damage that may be compensated – like the §823(1) of the German Civil Code (BGB) does – but use elastic clauses, such as «unjust harm», to allow the expansion of compensable damages. Such a clause has allowed the Italian Corte di Cassazione (Cass. civ., Sez. Un., 11 novembre 2008, n. 26972 Cass. civ., Sez. Un., 11 novembre 2008, n. 26973 Cass. civ., Sez. Un., 11 novembre 2008, n. 26974 Cass. civ., Sez. Un., 11 novembre 2008, n. 26975) and Constitutional Court (Corte Cost., 30 giugno 2003, n. 233; Corte Cost., 30 giugno 2003, n. 233, available online.org/decisioni/2003/0233s-03.html, last accessed June 10th 2020) to conclude that the minimal protection of the fundamental at http://www.giurcost rights of the individual – as put forth by the Italian Constitution – is granted through tort law. Thence, anyone who suffered a violation of his fundamental rights ought to be entitled to compensation from the tortfeasors if such harm was unjustified, leading to the compensation of non-pecuniary losses. On this matter, see Navarretta, E. (2009). L'ingiustizia del danno e i problemi di confine tra responsabilità contrattuale ed extracontrattuale. Diritto civile. N. Lipari and P. Rescigno. Milan, Giuffrè. III, IV: 233-253.

[241] European Commission (2017). SWD(2017)350. Commission Staff Working Document. Better Regulation Guidelines. Brussels.

The major concern for any liability system should be that of ensuring victim compensation, overcoming failures in the legal system such as those occurring in alternative causation scenarios, that are instead expected to increase in relevance and frequency due to technological complexity and opacity (§ 4.7.3).

To this end, identifying a single entry point for all litigation – according to a one-stop-shop approach (see § 4.7.4 below) – appears to be more efficient a solution, to be coupled with secondary litigation rights to allow the distribution of the risks along the entire value chain.

This in turn, requires the specific identification of a single responsible party towards the victim, who is best identified in relation to a given class of application, and not by resorting to a broad umbrella term, encompassing multiple agents (co)operating in the same context (see § 4.7.5).

Clarity and legal efficiency in ensuring victim compensation increases users' trust in technology, strongly favouring its uptake to the advantage of the industry, the economy and society overall (§ 4.7.6).

Also liability caps are best designed – when necessary – with respect to a specific kind of technological application, to ensure proportionality between harm suffered and compensation achieved is maintained (§ 4.7.6).

Overall, a technology-specific approach appears to be more coherent with that maintained up until today at European and MS's level alike, when regulating liability. Indeed, if different domains are separately addressed – e.g.: medical liability, traffic accidents, employer's liability, parents', teacher's, owners' and guardians' liability, and so on and so forth – technological development and the use of AI in those fields appears insufficient an argument to change such an approach (§ 4.7.1, § 4.7.6).

# 5. A RISK-MANAGEMENT APPROACH TO THE REGULATION OF CIVIL LIABILITY IN AI-BASED APPLICATIONS

**A Risk-Management Approach (RMA) as a technology-specific alternative to the regulation of advanced technologies**

52. A RMA is alternative to a technology neutral approach to regulating civil liability of new technologies [§ 5.2].
53. However, in accordance with other – even technology-neutral – proposals considered before [§ Ch 4], the RMA burdens a party who is in control of a given risk, best positioned to manage it.

**The RMA**

54. To regulate technology under a RMA, a three- step methodology is required: (i) a class of applications shall be identified that is sufficiently uniform, presenting similar technological traits, as well as corresponding legal, social, and economic concerns; (ii) applicable EU and MS legislation shall be assessed, according to the incentives, as well as the potential legal and market failures it may cause (prevent effective protection and appropriate costs-internalization, hamper innovation); (iii) when legal reform is needed, a proposal might be formulated [§ 5.2].
55. Liability rules should be specific for a given technology, pursuant to class-of-application-by-class-of-application approach [§ 5.2].
56. Liability rules should aim at ensuring prompt, full and effective compensation [§ 5.2].
59. Liability rules should burden the subject who is best position to (i) identify the risk, (ii) control it, (iii) and manage it, ensuring easy, prompt and full compensation to the victim, irrespective of considerations of fault [§ 5.2].
57. The responsible party does not necessarily bear the overall economic consequences of the accident. Indeed, through price and other market mechanisms he can transfer it onto all the users of a technology or service (pooling and spreading effect) [§ 6.2]. Through secondary litigation (rights to sue in recourse) and contractual agreements, he can distribute the loss along the entire value chain, yet minimizing primary litigation [§ 5.2].
58. The party to be held responsible will vary according to the different kinds of technological applications considered, in light of their complexity and functioning, as well as the way incentives are shaped (e.g. the operator of drones, the producer or owner of autonomous vehicle). This mechanism is consistent with some already enacted EU rules, such as the consumer sales directive, which grants immediate redress to consumers, by burdening the seller, *prima* facie, avoiding complex litigation [§ 5.2].
59. To make higher risks more manageable, first- or third-party – compulsory insurance might be adequate. Where compulsory insurance may have chilling effect (e.g. because lack of sufficient data lead to market failures) automatic no-fault compensation funds, or technology-specific liability caps may be considered [§ 5.2].
60. When multiple parties contribute to providing an AI-based service, making it hard to disentangle their roles, and to identify the optimal entry point for litigation, the creation of a fictive «electronic person» might be considered, if no other option is preferable [§ 5.2].

**Case study (i): industrial robots (IR).**

61. The legal framework on IR deriving from EU and MS law is adequate under a RMA, because: (i) victims benefit from prompt and adequate compensation, through workers' health and safety legislation, and the related national insurance system; (ii) business-users may sue, directly or in regress, other subjects of the production chain, on a contractual basis; (iii) the application of the PLD is residual and limited to business-users vs producers claims [§ 5.4].

**Case study (ii): connected and automated driving (CAD)**

62. As for CAD, the legal framework deriving from EU and national law is not adequate under a RMA, because (i) increasing automation causes the PLD and national traffic liability rules to overlap; (iii) apportioning liability becomes problematic, and exacerbates the major criticalities that the PLD displays; (iii) imposing duties to insure is per se insufficient, since it is not clear which party bears what risk. Ad-hoc legislation should be adopted at EU level, to burden the party that is best positioned to insure and minimize risks, through strict liability rules. These could likely be identified either in the owner or manufacturer of the vehicle, with partially different effects on the technology that will prevail [§ 5.5].

**Case study (iii): medical diagnostic assistive technologies**

63. As for medical diagnostic assistive technologies, the legal framework deriving from EU and national law is not adequate under a RMA, because: (i) sees an overlap of product liability legislation and, national provisions on medical malpractices, which are either contractual or tortious, and hold the doctor/hospital liable in case of professional negligence; (ii) leads to defensive medicine practices. Existing liability rules should be revised as to shield doctors from direct responsibility connected to the use of medical systems, and rather hold either the hospital, or the producer, liable either through strict liability rules, or by establishing a form of enterprise-liability for service providers [§ 5.6].

**Case study 4: drones**

64. As for drones, the legal framework deriving from EU and MS law is partly adequate under a RMA, because: (i) MS laws tend to converge on holding the operator (or the owner) strictly liable for failing to ensure the safety of drones' operation; (ii) set third-parties compulsory insurance, differentiating on the basis of the mass and use of the devices; (iii) however, overlap with the PLD and other liability regimes may lead to possible uncertainties and alternative causation scenarios. A EU regulatory intervention, even with respect to liability, is therefore advisable to achieve maximum harmonization among MS, yet it is not a pressing necessity [§ 5.7].

## 5.1. A Risk-Management Approach to civil liability

All efforts at regulating civil liability for harm arising from the use of AI-based applications and advanced technologies address two fundamental aspects, product liability rules and the possibility of conceiving ad-hoc regulation; both options are typically considered working in parallel, and thence not as mutually exclusive.

For this reasons, a series of solutions have been taken into consideration at the EU level, from a revision of the PLD, to the discussion on possible draft regulation on AI technologies[242] (Ch. 3, § 3.5 and Ch. 4,

[242] Committee on Legal Affairs (2020). Draft Report with recommendations to the Commission on a Civil liability regime for artificial intelligence (2020/2014(INL)), European Parliament.

§). Quite commendably, the most important and recent proposal commit, either implicitly or explicitly, to a RMA.

As for the PLD applies, all commentators, including the EG, point at the overall weaknesses of the current system of producer's liability, as emerging from its implementation at EU level, and suggest modifications that despite useful for all other applications, appear of essential importance when advanced technologies are considered (see Ch. 3, § 3.5, and Ch. 4, § 4.2). Suggested interventions primarily entail reforming defences (including eliminating the development risk defence), redefining causation (either through substantive law solutions or procedural ones), and defectiveness, reconsidering the notion of product and its distinction with services. So modified, the PLD would become a profoundly different piece of legislation, and converge towards a RMA.

As for the adoption of ad-hoc liability rules, proposals advanced towards the adoption of ad-hoc liability rules, such as the EG considerations on operators' liability (see Ch. 4, § 4.6.7), identify possible responsible parties primarily on functional grounds, because they control a risk associated with the AI-system, and may be the first visible contact point for the affected person.

However, these proposals and studies either expressly commit to an idea of technological neutrality[243] (critically discussed in Ch. 4, § 4.3), or adopt such broad and general criteria both for determining their scope of application and for elaborating the relevant liability regime, that, in practice, present the same criticalities of the one-size-fits-all solution they claim to reject[244].

Indeed, it is indisputable that advanced and AI-based technologies differ profoundly among one another[245], first of all on technical grounds. There is no similarity between an expert system used in medical diagnosis, and an electronic toothbrush; between a collaborative industrial robot (or co-bot), and a health-app; a facial-recognitions system and a smart-thermostat; a driverless vehicle and a chatbot, to name a few well-known examples. Yet, all such applications would fall under the broad umbrella term of AI-based applications.

Looking for commonalities is a futile exercise, doomed to fail on technical grounds, but also in a social science and regulatory perspective. Indeed, even the ethical and legal implications they give rise to, and the solutions they might require differ as profoundly. In most cases, no legal intervention is necessary. In others, instead, it seems unavoidable, and yet such intervention should consist in the adoption of specific solutions, that consider those relevant specificities that are not merely technical – the kind of AI-application and function they are grounded upon – but also dependent upon (i) the use made, (ii) the fundamental rights it impacts upon or contributes to satisfy, (iii) the nature of the party using and benefitting from it – professional or not –, (iv) the size of the potential market, and the clear identification of potential market failures, (v) also connected to the potential availability of adequate insurance products.In such a perspective, all proposed solutions, to be relevant and future proof, and

[243] (2018). Commission Staff Working Document Evaluation of Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products SWD(2018) 157 final Brussels, European Commission, Ernst&Young, Technopolis and VVA (2018). Evaluation of Council Directive 85/374/EEC on the approximation of laws, regulations and administrative provisions of the Member States concerning liability for defective products. Brussels, European Commission.

[244] Expert Group on Liability and New Technologies - New Technology Formation (2019). Report on Liability for Artificial Intelligence and other emerging digital technologies.

[245] Bertolini, A. (2013). "Robots as Products: The Case for a Realistic Analysis of Robotic Applications and Liability Rules." Law Innovation and Technology 5(2): 214, Bertolini, A. and E. Palmerini (2014). Regulating Robotics: a Challenge for Europe. Upcoming Issues of EU Law, available at http://www.europarl.europa.eu/document/activities/cont/201409/20140924ATT89662/20140924ATT89662EN.pdf. D.-G. f. I. Policies. Bruxelles.

to minimize legal uncertainty – thus easing technological development and the flourishing of its connected industry[246] – need to be technology-specific.

After all, if AI is pervasive of most if not all of the fields of human activities (as exemplified above), regulation, in order to be effective and useful, needs to reflect that diversity. Said otherwise, if up until today medical liability is not regulated unitarily and identically with the liability of intermediaries operating in financial markets, of distributors of consumer goods, of nuclear-power-plants operators, car owners and drivers, internet service providers, employers in industrial settings, and so on and so forth, there is no clear and evident reason why the introduction of AI-based solutions in all such domains should radically change the regulatory approach so far maintained by policy-makers all over the world.

It is therefore evident how proposed umbrella-definitions of AI-based applications even when classified through very broad distinctions – such as the high- v.s. low-risk one (see Ch. 4, § 4.7.2 above) – depart from such an approach, giving rise to the concerns analytically discussed.

A preferable approach should thence be technology-specific, and address classes of applications characterized by evident similarities in their design, and functions, as well as in the regulatory concerns they give rise to, in light of the criteria enumerated above, (i) to (v).

Therefore, before proceeding with the analysis of some applications that might be deemed of particular relevance due to their (i) novelty, (ii) expected impact and (iii) diffusion[247] – see § 4.6.3 and § 4.7.2 –, some fundamental theoretical (see § 5.2) and methodological (see § 5.3) considerations need to be drawn.

## 5.2. A Risk-Management Approach: theoretical considerations

The RMA attributes liability to the party that is best positioned to (i) identify a risk, (ii) control and minimize it through its choices, and (iii) manage it – ideally pooling and distributing it among all other parties – eventually through insurance, and/or no-fault compensation funds. To do so, it resorts to strict – if not absolute – liability rules.

In this respect it differs from a fault-based liability rule because it does not attempt to reprehend the party held liable for having departed from an intended conduct. Ultimately, the party being held liable might not be blameworthy, and more specifically it might be hard to pinpoint a conduct that might be deemed wrong, having directly affected the victim.

Indeed, said approach moves from the basic and empirical consideration that liability rules are not always effective in providing *ex ante* incentives towards maintaining a desirable conduct – such as in the case of driver's responsibility in road circulation – or making an adequate safety investment – such as in the case of producers' liability –[248]. Frequently, market mechanisms on the one hand – e.g.:

[246] Expert Group on Liability and New Technologies - New Technology Formation (2019). Report on Liability for Artificial Intelligence and other emerging digital technologies. Committee on Legal Affairs (2020). Draft Report with recommendations to the Commission on a Civil liability regime for artificial intelligence (2020/2014(INL)), European Parliament.

[247] These criteria for selecting technologies to be regulated were first exemplified and discussed by the conclusions of the Robolaw project; see Palmerini, E., F. Azzarri, F. Battaglia, A. Bertolini, A. Carnevale, J. Carpaneto, F. Cavallo, A. Di Carlo, M. Cempini, M. Controzzi, B.-J. Koops, F. Lucivero, N. Mukerji, L. Nocco, A. Pirni, H. Shah, P. Salvini, M. Schellekens and K. Warwick (2014). Guidelines on Regulating Robotics. Robolaw Grant Agreement Number: 289092, D6.2.

[248] See Posner, R. (2007). Economic Analysis of Law, Wolters Kluwer. 182; Polinsky, M. A. and S. Shavell (2009-2010). "The uneasy case for product liability." Harvard Law Review 123: 1437, Helland, E. A. and A. Tabarrok (2012). "Product Liability and Moral Hazard: Evidence from General Aviation." The Journal of Law and Economics 55: 593, Bertolini, A. (2013). "Robots as Products: The Case for a Realistic Analysis of Robotic Applications and Liability Rules." Law Innovation and Technology 5(2): 214, (2018). Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01), Article 29 Data Protection Working Party: 8.

reputation – and detailed *ex ante* applicable regulation, such as product safety rules (see Ch. 3, § 3.1) are much more effective towards that end.

In such a perspective, the primary purpose of liability rules should be that of ensuring victim compensation. Failures in the legal system might cause victims not to receive compensation even when they would be entitled to, that is whenever they suffer a loss that is unjust – as it corresponds to the violation of one of their rights or legally relevant interests – absent an adequate legal justification – e.g.: the responsible party did not act in self-defense or enacting one of her own fundamental rights (e.g.: freedom of speech) –[249] and they did not cause their own damage.

Undercompensating victims is a serious failure of the legal system, allowing the parties that benefit from an activity, service or good – who could be doing so for both professional and personal reasons, as producers or service providers, as well as users of a given product or service – not to internalize the costs they generate upon society, eventually leading to distortive effects in the market and competition (see also Ch. 4, § 4.3 above).

Such an approach is essential when advanced AI-based applications are considered. Indeed, due to their opacity and complexity[250], and the circumstance that multiple parties collaborate in providing a good or service, leading to the overlapping of different liability regimes, and conducts that are not always easily and cheaply analyzed to identify the relevant causal factor, the risk of undercompensating victims is a serious concern[251].

It shall be stressed, that both MS and the European legal systems admit liability rules that abide such rationale, both through strict and vicarious liability rules[252].

Victims facing too high litigation costs due to both technological complexity and legal inefficiency, would either not sue – and bear themselves the negative consequence of the accident – or sue the weaker link – possibly another user of private owner of the technology, e.g.: the owner of a driverless car – in any case preventing an appropriate internalization of costs by those that control the risks and benefit from them.

To favour access to justice – that might otherwise be *de facto* denied – and also a more correct internalization of costs by those who are best positioned to control them and most directly benefit from them, it is also essential to clearly identify the party who, *prima facie*, should be called in to compensate the damage suffered, leaving to price mechanisms (see also § 5.5), secondary litigation and contractual agreements the role of distributing those costs along the value chain and all other subjects involved[253].

Indeed, complexity, opacity and the collaboration of multiple parties might give also rise to a large number of cases of «alternative causation», whereby it is not obvious which one factor – if indeed one prevailed – led to the harmful outcome, potentially preventing the victim from rightfully achieving compensation. *Vis a vis* such kind of uncertainty litigation costs for the victim would certainly rise – should she decide to sue all of the potentially involved parties – and most likely discourage access to justice in a relevant number of circumstances – for even when facing litigation the outcome would be

[249] Navarretta, E. (2009). L'ingiustizia del danno e i problemi di confine tra responsabilità contrattuale ed extracontrattuale. Diritto civile. N. Lipari and P. Rescigno. Milan, Giuffrè. III, IV: 233-253.

[250] Expert Group on Liability and New Technologies - New Technology Formation (2019). Report on Liability for Artificial Intelligence and other emerging digital technologies., EG's key finding nn°1, 5.

[251] Bertolini, A. (2016). "Insurance and Risk Management for Robotic Devices: Identifying the Problems." Global Jurist(2): 1-24.

[252] For a broad exemplification and account see Expert Group on Liability and New Technologies - New Technology Formation (2019). Report on Liability for Artificial Intelligence and other emerging digital technologies., 23-29.

[253] See also EG, 55-59. Bertolini, A. (2016). "Insurance and Risk Management for Robotic Devices: Identifying the Problems." Global Jurist(2): 1-24.

most uncertain, since no one of the defendants might be obliged to compensate – ultimately negatively affecting the very decision to adopt a more advanced technology (see also § 5.5).

This problem is therefore best addressed by identifying *ex ante* a single, clear and unquestionable, entry point for all litigation, according to a one-stop-shop approach.

Therefore, among the possible parties that could benefit from the use of a technology, and who are in the position to identify and control risks, one should be selected, who is held responsible towards the victim on strict – if not absolute – grounds.

This party will certainly vary according to the different kinds of technological applications considered, in light of their complexity and functioning, as well as the way incentives are shaped. For instance, in some cases, it may be appropriate to hold primary responsible the operator (e.g. drones) the business user and/or system integrator (advanced industrial robots), the service provider or deployer (AI-based consultancy services), the hospital and/or medical structure, and/or service provider (in case of medical diagnosis), the producer and/or the owner (in increasingly autonomous vehicles; for an analysis of these different types of liability, see §§ 5.4-5.7 below)

It shall be noted that the party who is called in to compensate damages in the first place is not necessarily the party who ultimately bears the economic consequences of the accident. Indeed, market mechanisms – above all price – allow the burdened party to estimate the cost of liability – even more so when resorting to insurance coverage to transform *ex post* uncertainty into a defined *ex ante* cost – and transfer it to all users, who benefit from a product or service. Moreover, rights to act in recourse – in secondary litigation – as well as contractual agreements[254] would allow the party who compensated the victim to more efficiently internalize and then distribute the costs along the entire value chain, to the party that is specifically in control of the one risk that materialized (see § 5.5).

Such a solution would minimize first level litigation between the victim and the sole clearly responsible party, favouring access to justice, and eradicating the risk of under compensation, also due to alternative causality scenarios. Moreover, minimizing litigation costs favours the legal system overall – preventing excessive burden for the MS' and European court system – as well as for the industry.

Even such mechanism is not foreign to European law. Indeed, the Consumer Sales and Guarantees Directive (CSGD), represents a very positive and effective example of such rationale, that contributed to the effective protection of European consumers, without forcing them to resort to complex litigation. Pursuant to art. 3 of the CSGD, consumers who receive a defective product – non-conforming with the contract of sale (art. 2.1 CSGD) – are entitled to act directly against the seller, to have it repaired, or replaced, or eventually to receive the restitution of the full purchase price or of a portion thereof. Even if it is clear that in the vast majority of cases the seller has no direct control over product quality, and thence might not be deemed responsible for its lack of conformity, he is the most effective entry point to ensure consumers receive what they are entitled to, without the need for litigation. Then, the reseller will be allowed to act in recourse against the manufacturer with whom he is in contractual business relationships.

The very positive experience of this directive could be used as a potential model also for the regulation of advanced technologies, such as those here considered.

Alternatively, when multiple parties contribute to providing a complex and opaque AI-based product or service, and disentangling their roles might appear ever more difficult, as well as identifying the optimal entry point for litigation, the creation of a fictive legal entity – a legal or electronic person –

[254] See Expert Group on Liability and New Technologies - New Technology Formation (2019). Report on Liability for Artificial Intelligence and other emerging digital technologies., 57-59.

might serve the identical purpose (see Ch. 2, § 2.3). A similar approach might be preferable when AI-based services are considered, rather than products sold. Said otherwise, it would certainly not be an adequate solution for driverless cars, maybe, under certain conditions, non-embedded AI solutions used in consultancy or to operate on capital markets. The rationale, in such cases, would be identical to the one just described, for the new legal entity would see the participation of all the different parties involved in providing the service, who ultimately would bear the economic consequences of liability according to their share of interest in the entity itself[255].

Finally, in some cases, in order to make higher risks more manageable, different approaches might be utilized including – first- or third-party – compulsory insurance[256] , automatic no-fault compensation funds[257], and liability caps, differently combined.

It shall however be noted that compulsory insurance is not always an ideal solution. In some cases – in particular absent legal reform – legal risks might be hard to define – in case of multiple potential tortfeasors and the absence of clear-cut liability rules of the kind here suggested – as well as the empirical ones. The absence of statistically relevant data, the difficulty in identifying ex ante unknown-unknown risks, and in assessing their probability, as well as the limited market for one specific class of applications[258] (see Ch. 4, § 4.6.3 and fn.203), might cause the offering of adequate insurance products to be problematic. Thence, a duty to insure might cause a strong technology chilling effect, and thence the alternative of providing for an automatic compensation fund – financed through ad-hoc taxes/fees imposed on the (i) producers, and/or (ii) service providers, and/or (iii) users of product or service or through public spending – typically coupled with damage caps and limitations could be reconsidered.

Finally, damage caps and limitations, if provided, should be proportionate to the specific risks a given class of applications gives rise to, that might typically differ from those triggered by a different one. This is indeed, another argument in favour of technology-specific regulation.

## 5.3. A Risk-Management Approach: methodological considerations

The theoretical criteria described above (see § 5.2) need to be applied to identified classes of technological applications, that appear to require ad-hoc regulation on the basis of a fundamental assessment, here described.

Firstly, a class of applications needs to be identified that is sufficiently uniform, presenting similar technological traits, as well as corresponding legal – and in some cases ethical – concerns. In such a perspective a drone differs from a driverless car. They both are intended to operate in public spaces, and display some degree of autonomy. Yet the technologies they are based upon differ, the environment they will be used in as well, the dynamic of the possible accidents too. Moreover, their use, their social role, and potential diffusion also varies, and so do the parties that might be involved in their operation, and the structure of the business through which services might be offered.

Non-embedded expert systems used for diagnosis differ under all such aspects even more from the previously mentioned technologies, as well as they differ from industrial robots, despite both being

---

[255] Bertolini, A. (2016). "Insurance and Risk Management for Robotic Devices: Identifying the Problems." Global Jurist(2): 1-24, Palmerini, E. and A. Bertolini (2016). Liability and Risk Management in Robotics. Digital Revolution: Challenges for Contract Law in Practice. R. Schulze and D. Staudenmayer. Baden-Baden, Nomos: 225-259.

[256] Expert Group on Liability and New Technologies - New Technology Formation (2019). Report on Liability for Artificial Intelligence and other emerging digital technologies., 61-62.

[257] Ibid., 62 -63.

[258] See for instance the case of biorobotics applications for amputees Bertolini, A. (2015). "Robotic prostheses as products enhancing the rights of people with disabilities. Reconsidering the structure of liability rules." International Review of Law, Computers & Technology 29(2-3): 116-136.

operated in what could be deemed as «private spaces»[259], and by parties that might be involved in a contractual relationship one with the other.

Then, extant legislation – at MS and EU level, when relevant – needs to be identified that could be specifically applied to the class of applications, and a prospective – when the technology is not yet widely diffused – functional analysis of the incentives it gives rise to and potential legal and market failures it may cause needs to be undergone.

Finally, based on the theoretical criteria discussed above (see § 5.2) grounding a RMA, when legal reform is needed, and only in such cases, a proposal might be formulated, whereby one specific party is clearly held responsible, pursuant to strict – if not absolute – liability rules, as sole entry point for all litigation, granting rights to act in recourse, imposing – when appropriate – duties to insure, and eventually capping liability.

Overcoming an ill-understood technological neutrality that does not pertain either to the MS' or to the European legal systems, such a bottom-up, and functional analysis might lead to conclude that no specific intervention is needed in one case (see for instance industrial robots § 5.4 below), while in other cases it might justify elaborating proposals where one party (e.g.: operator, for drones) ought to be responsible, that differs in other cases (e.g.: owner or producer, for driverless cars).

## 5.4. Industrial Robots

### 5.4.1. Definition and description of the relevant features

Technological innovation is profoundly affecting production techniques[260], and the very conception of what a factory is, how it is structured, and how it functions. Such a phenomenon is referred to as the fourth industrial revolution, or Industry 4.0[261], and entails, among other things, the evolution of traditional plants into smart factories[262], i.e. manufacturing environments where cyber-physical systems and robots operate with various degrees of autonomy[263], and interact with human beings, often moving freely outside restrained spaces. Industry 4.0 solutions are cooperative, intended to function in direct contact with the user, and, in some cases, be worn, such as exoskeletons.

Given their wide application in this new environments, their importance for the European industry, and the potential risks connected to the unrestrained and continuous contact with humans – potentially endangering bodily integrity, as well as other fundamental rights (e.g. privacy)[264] – such advanced and AI-based robotics constitute a class of application that policy makers may want to monitor closely, to ensure that they are adequately regulated.

[259] As stated by the EG, «strict liability is an appropriate response to the risks posed by emerging digital technologies, if, for example, they are operated in non-private environments and may typically cause significant harm». See Expert Group on Liability and New Technologies - New Technology Formation (2019). Report on Liability for Artificial Intelligence and other emerging digital technologies., EG's key finding nn°9, 6. But please allow us to refer to the critical considerations already drawn in that respect under Ch. 4, § 4.6.3 and § 4.7.1.

[260] Davies, R. (2015). Industry 4.0 Digitalisation for productivity and growth, European Parliament.

[261] Till, A. L., S. Zahidi and V. Ratcheva (2016). The Future of Jobs Employment, Skills and Workforce Strategy for the Fourth Industrial Revolution, World Economic Forum.

[262] Communication Investing in a Smart, Innovative and Sustainable Industry. A Renewed Eu Industrial Policy Strategy (European Commission, 2017). Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee, the Committee of the Regions and the European Investment Bank, Investing in a smart, innovative and sustainable Industry. A renewed EU Industrial Policy Strategy, September 13th, 2017.

[263] Smit, J., S. Kreutzer, C. Moeller and M. Carlberg (2016). Industry 4.0, European Parliament.

[264] For a detailed analysis see Timan, T., R. Snijders, M. Kirova, S. Suardi, M. v. Lieshout, M. Chen, P. Costenco, E. Palmerini, A. Bertolini, A. Tejada, S. v. Montfort, M. Bolchi, S. Alberti, R. Brouwer, K. Karanilokova, F. Episcopo and S. Jansen (2019). Study on safety of non-embedded software. Service, data access, and legal issues of advanced robots, autonomous, connected, and AI-based vehicles and systems: final study report regarding CAD/CCAM and industrial robots. Brussel, European Commission., Annex 3, 82 -93.

However, IR themselves constitute a heterogeneous and constantly evolving category, encompassing a wide array of applications[265]. Thus, it is necessary to identify specific applications to be singularly discussed.

Indeed, this paragraph discusses three types of IRs, which stand out because of the novelty of their application, as well as their AI-based functioning: (i) collaborative robots, i.e. «robot[s] designed for direct interaction with a human»[266], (ii) mobile robots, i.e. «robot[s] able to travel under [their] own control» both «with or without manipulators»[267], and (iii) exoskeletons, i.e. external structural mechanism with joints and links corresponding to those of the human body.[268]

These three types of applications, despite having their own peculiarities, may be treated as a single class of applications because they share the same features and characteristic of use. In particular, they all display high degrees of automation and they are all used within an environment which is not open to the general public (the smart factory). To operate, they are normally either produced by or – most commonly – bought by business users (the company running the smart factory), and are identified, customized and installed by them with the help of system integrators. Moreover, they are all operated by specific – and most commonly trained – subjects (factory workers and operators), and interact either directly or indirectly with the same kind or professional workers (namely, the very worker operating them, co-workers interacting with them, or by-stander co-workers).

### 5.4.2. Existing legal framework

When discussing liability of IR, two different bodies of law shall be analyzed, concerning, respectively: (i) health and safety of workers, and the relevant insurance or pension schemes; (ii) compensation for damages caused by IRs, under general private law contractual or tortious rules, as well as the specific product liability regime set up by the PLD and its national implementation. The linchpin for the two bodies of law is the business-user who is, in fact, at the same time the purchaser of the technology – entering into a sale and service contract with the other business players herein considered, i.e. manufacturers and system integrators –, as well as the subject responsible for the safety of workers on the workplace.

The first body of law encompasses the business-users' responsibility and liability towards its employees as victims of the use of IRs. Business-users are subjects responsible for the safety of workers on the workplace under the EU and MS' legal framework, which is applicable also in case of damages caused by IRs. European legislation consists of the Framework Directive 89/391/EEC [269] (WFD) and other adjacent directives and regulations on the most significant issues related to safety in the workplace [270].

---

[265] International standards, namely ISO 8373:2012, define IRs as «automatically controlled, reprogrammable, multipurpose manipulator, programmable in three or more axes, which can be either fixed in place or mobile for use in industrial automation applications» https://www.iso.org/obp/ui/#iso:std:iso:8373:ed-2:v1:en (last accessed June 29th 2020).

[266] ISO 8373:2012, ISO 10218-2:2011;

See https://www.iso.org/obp/ui/#iso:std:iso:8373:ed-2:v1:en, See https://www.iso.org/standard/41571.html, (last accessed June 29th 2020).

[267] ISO 8373:2012, ISO 19649:2017. See https://www.iso.org/obp/ui/#iso:std:iso:8373:ed-2:v1:en (last accessed June 10th 2020). Also see the definition of Automated Guided Vehicles which is a sub-category of mobile robots defined under ISO 8373:2012, 3.20 «a mobile platform (3.18) following a predetermined path (4.5.4) indicated by markers or external guidance commands, typically in the factory. See https://www.iso.org/standard/65658.html, (last accessed June 29th 2020).

[268] See, for personal care robots, ISO 13482:2014 https://www.iso.org/standard/53820.html(last accessed June 29th 2020).

[269] Council Directive 89/391/EEC of 12 June 1989 on the introduction of measures to encourage improvements in the safety and health of workers at work, in OJ L 183, of June 210th, 1989.

[270] In this respect see: (i) Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast) (Text with EEA relevance) OJ L 157, 9.6.2006; (ii) Regulation (EU) 2016/425 of the European Parliament and of the Council of 9 March 2016 on personal protective equipment and repealing Council Directive 89/686/EEC, in OJ L 81, of March 31st, 2016; (iii) Council Directive 89/686/EEC of 21 December 1989 on the approximation of the laws of the Member States relating to personal protective equipment, OJ L 399, of December 30th, 1989; (iii) Directive 2009/104/EC of the European Parliament and of the Council of 16 September 2009 concerning the minimum safety and health requirements for the use of work equipment by workers at work (second individual Directive

The WFD provides for a wide range of statutory safety-related duties (art. 5 WFD), namely: (i) prevention of occupational risks and provision of information to and consultation with workers– by ensuring that the planning and introduction of new technologies are subject to consultation with the workers and/ or their representatives – and training so as to ensure that each worker receives adequate safety and health related instruction in the event of the introduction of any new technology (art. 6 and art. 12 WFD), and (ii) implementation of a risk-management measure including avoiding, evaluating, minimizing and combating risks, giving appropriate indications, implementing prevention policies, etc. (art. 6 WFD).The sanctions applicable for the breach of said statutory duties are regulated at MS' level and are comprised of a combination of civil, criminal and administrative liability[271].

Furthermore, although the current EU framework on health and safety of workers at the workplace does not provide for any form of compulsory insurance, some MS, such as Austria[272], Spain[273] and France[274], do.

Under this framework, a worker who suffers damage while operating, or interacting with an IR (operated by a co-worker, or autonomous), would obtain compensation though social security schemes or by addressing a contractual or tortious claim against the employer. Most importantly, compensation would be ensured in all cases, regardless of whether the damage was caused by the negligence of the co-worker, or by the victim's own conduct, and irrespective of the safe or defective nature of the IR in question.

Even if the victim happened to be an occasional non-worker by-stander, the latter may be able to claim compensation based on MS' liability rules, under different tort doctrines and civil law principles that allow for redress (e.g. vicarious liabilityand/or *Schutzpflichten*).

The second body of law, instead, covers the liability of producers and systems integrators for damages caused by defective IR, and consists of the PLD, and national contract and tort law. Here, the type of damages addressed are those suffered by business-users either directly, as a consequence of the malfunctioning of a defective robot (e.g. damage to the smart-factory property), or indirectly, i.e. when acting in recourse after having been obliged to compensate the workers under the scenario described above.

Indeed, given the efficacy of the employer's liability discussed above, it is unlikely that the victim would rely on any other ground of liability – should the damage be caused by a defective IR – to obtain compensation. In this sense, this second framework rather offers redress mechanism for the business-

within the meaning of Article 16(1) of Directive 89/391/EEC), in OJ L 260, of October 3rd, 2009; and (iv) Council Directive 89/654/EEC of 30 November 1989 concerning the minimum safety and health requirements for the workplace (first individual directive within the meaning of Article 16 (1) of Directive 89/391/EEC), in OJ L 393, of December 30th, 1989.

[271] This is the case in Italy as under D. Lgs. April 10th, 2008, n. 81 «in materia di tutela della salute e della sicurezza nei luoghi di lavoro» all subjects in charge of guaranteeing safety may be subject to civil, administrative, and criminal liability. Similarly, the French Code du Travail Criminal provides for criminal and administrative liability for employers under art. L4741 to L4754. Also, see the comprehensive assessment of the MS legislation in this respect in Timan, T., R. Snijders, M. Kirova, S. Suardi, M. v. Lieshout, M. Chen, P. Costenco, E. Palmerini, A. Bertolini, A. Tejada, S. v. Montfort, M. Bolchi, S. Alberti, R. Brouwer, K. Karanilokova, F. Episcopo and S. Jansen (2019). Study on safety of non-embedded software. Service, data access, and legal issues of advanced robots, autonomous, connected, and AI-based vehicles and systems: final study report regarding CAD/CCAM and industrial robots. Brussel, European Commission., Annex 3, 86-88.

[272] Bundesgesetz vom 9. September 1955 über die Allgemeine Sozialversicherung (Allgemeines Sozialversicherungsgesetz – ASVG.) StF: BGBl. Nr. 189/1955 idF BGBl. Nr. 18/1956 (DFB) (NR: GP VII RV 599 AB 613 S. 79. BR: S. 108.), available at the following link: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=1000847 (last accessed June 29th 2020).

[273] Ley 42/2006 de 28 de diciembre - P.G.E. 2007, available at the following link:
http://www.segsocial.es/wps/portal/wss/internet/Trabajadores/CotizacionRecaudacionTrabajadores/10721/10957/583#582 (last accessed June 29th 2020).

[274] Décret n°85-1354 du 17 décembre 1985 Relatif Au Code De La Securité Sociale. For a more comprehensive view see Timan, T., R. Snijders, M. Kirova, S. Suardi, M. v. Lieshout, M. Chen, P. Costenco, E. Palmerini, A. Bertolini, A. Tejada, S. v. Montfort, M. Bolchi, S. Alberti, R. Brouwer, K. Karanilokova, F. Episcopo and S. Jansen (2019). Study on safety of non-embedded software. Service, data access, and legal issues of advanced robots, autonomous, connected, and AI-based vehicles and systems: final study report regarding CAD/CCAM and industrial robots. Brussel, European Commission., Annex 3, 90

user, who may be claiming damages arising from the use of defective products acting against the IRs producer. Since, IRs – like many of new technologic-advanced applications (Ch 3, § 3.4.1) – qualify as products under art. 2 of the directive, both the manufacturer, service providers, and system integrators could – under different conditions – be held liable, all qualifying as «producers» for the purposes of art. 3, PLD, either separately or jointly and severally, depending on a case-by-case assessment of their contribution to the final design of the production line. From a RMA perspective, the PLD redress is deemed effective with respect to a business user's right to recover damages for defective IRs, also considering the professional nature and expertise of the parties involved, and the information available to both.

Indeed, a claim for damages under the PLD may constitute an even more convenient way of seeking redress, as the allocation of risks and responsibilities among parties would be pre-determined in the contract, making it easier to establish and assess the breach[275]. Furthermore, even if no actual redress is sought, the liable party will be able to (re)negotiate their contractual agreements with her business counterparts to distribute the economic consequences of the malfunctioning along the entire value chain[276]. In this sense, the existence of the right to claim damages both under the PLD and under contract law, allows for a sufficient redress mechanism and legal framework and no responsibility gap can be identified herein so as to require the enactment of new legislation.

Furthermore, inefficiencies often associated with the enforcement of the PLD do not apply in the case at hand, given that business users and producers would be deemed professionals, with comparable bargaining power and access to information and technical expertise, relevant to demonstrate the existence of a defect – when that is the case – and of a causal nexus between that and the damage. The concerns often associated with the effectiveness of the PLD, such as the information asymmetry, would not be applicable.

### 5.4.3. Assessment and recommendations

Thus, the relevant legal framework on liability and insurance of IRs comprises two different bodies of law.

The first body of legislation consists of the Framework Directive 89/391/EEC (WFD), a series of further directives and regulations on safety at the workplace, and the national laws implementing them. Under MS' social system, workers benefit from compulsory insurance schemes or pensions covering job-related accidents.

The second body of legislation consists of the PLD, and the national laws implementing it, which display substantial differences among one another. As for other technological devices, the PLD offers insufficient protection to the victim, due to the difficulties in ascertaining and apportioning liability, as well as in proving the defect of the product and the causal nexus between the defect and the damage (see Ch. 3, § 3.4.2 and § 3.4.4 above). However, these problems do not arise in the case of IRs, at least not with the same degree of severity which comes about when other technologies and parties are involved.

[275] As showed under the PLD evaluation study, of the over 798 cases considered, in around 20% of the times the Courts ruled according to a legal basis different from the PLD. Among them, around two thirds of the cases were decided resorting to national contract law rules, and one fifth through the application of general tort law principles. See in this respect Ernst&Young, Technopolis and VVA (2018). Evaluation of Council Directive 85/374/EEC on the approximation of laws, regulations and administrative provisions of the Member States concerning liability for defective products. Brussels, European Commission.

[276] An exceptional case may be however envisioned whereby exoskeletons are purchased by the victim for personal use, in which case the existing concerns expressed with respect to the PLD and its enforcement by individual victims become applicable, such as information asymmetry, high costs and expertise required to prove the casual nexus, etc.

Further, due to the peculiar relationship between the subjects involved, the victim – the operator of the IRs, or a coworker – will not face any difficulty connected to the identification of the subject who is liable to compensate the damages, i.e. the employer, and will benefit from the compulsory insurance for accidents occurred at the workplace, thus being overall better off as opposed to those injured by other types of technologically advanced devices (e.g. drones – see in this respect § 5.7 below) .

Such mechanism is consistent with a RMA, as the subject who is held liable to pay for the damage is the one who is best positioned to (i) identify and manage the risk of its occurrence, thus adopting the most appropriate measure to prevent it, (ii) acquire insurance and thus manage the costs, once the damage has occurred, and finally (iii) redistribute such costs along the supply chain, when the damage is caused, for example, by a defect of the robots for which the manufacturer, or the system integrators, are responsible. Indeed, it is likely that the business user, who has been called in to compensate for the damaged suffered by one of his employee, decides to sue in recourse the aforementioned subjects, either to claim damages, or to re-negotiate the contractual agreement, as to make good for the expenses suffered.

To conclude, as far as liability is concerned, the current *status quo* is sufficient and does not require any intervention, since (i) the framework on health and safety of workers, and the related national insurance system, ease the position of the victim, who may benefit from prompt and adequate compensation; (ii) business-users may sue the other subject of the value chain, directly or in recourse, on a contractual basis; (iii) the application of the PLD remains residual, and thus problems which it arises for other technologies have only little practical relevance.

## 5.5. Connected and automated driving

### 5.5.1. Definition and description of relevant features

The underway development of smart cities[277], through the use of digital and telecommunication technologies, is about to bring many benefits to their inhabitants, such as more inclusive urban transport networks and better administered and safer public spaces. Automated driving (henceforth AD) represents one key element in the development of said smart cities, as recognized through many EU initiatives[278], such as the Communication from the Commission on the road to automated mobility, setting an EU strategy for the mobility of the future.

The envisioned benefits of AD solutions (henceforth ADS) are noteworthy, such as the increase of road safety through the elimination of the human error as a major cause of accidents.

Nevertheless, AD is not risk-free and the challenges it may pose to extant liability frameworks are varied. ADS are complex technological solutions functioning in a legal framework developed for traditional driving, from which they differ substantially. ADS differ among each other and from traditional vehicles with respect to their capabilities and features, as the control of the machine is granted to an automated pilot and not to the human – or the driving task is at least shared between the two – , and various players, with different levels of contribution, appear on the production, use and liability chain.

[277] See in this respect the EU initiatives on smart cities at https://ec.europa.eu/info/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart-cities_en.

[278] See in this respect: (i) the High Level Group GEAR 2030 initiative available at https://ec.europa.eu/growth/content/commission-launches-gear-2030-boost-competitiveness-and-growth-automotive-sector-0_en (last accessed June 29th 2020); (ii) the digital cross-borders corridors initiative undersigned by MS, available at https://ec.europa.eu/digital-single-market/en/cross-border-corridors-connected-and-automated-mobility-cam (last accessed June 29th 2020); (iii) the Cooperative Intelligent Transport Systems (C-ITS) initiative, - Communication. A European Strategy on Cooperative Intelligent Transport Systems, a Milestone Towards Cooperative, Connected and Automated Mobility (Brussels: European Commission, 2016); (iv) the C-ROADS Platform, available at https://www.c-roads.eu/platform/about/about.html, (last accessed June 29th 2020).

Despite its heterogeneous applications[279] the technological characteristics of ADS are reducible to: (i) autonomy, which may vary from no-automation (traditional driving), to full automation (where the human is a mere passenger and control is entirely vested upon the solution)[280] and (ii) internet connectivity allowing the vehicle to share internet access with other vehicles, infrastructure and devices, both inside as well as outside the vehicle[281]. For the purpose of brevity and comprehensiveness, this paragraphs will refer to a specific form of AD, i.e. connected and automated driving (CAD) – which are vehicles that have different degrees of automation (normally identified in a sale from 1 to 5 of the SAE)[282] and are connected with other vehicles, with the infrastructure, and/or with other devices – as they are located in the middle of the spectrum between traditional driving systems and particularly advanced and complex solutions, such as those represented by connected and cooperated automated mobility, and constitute the type of application which will most likely be available in the future.

This section will thus, describe the legislative framework applicable to CAD, both at EU and MS' level, assess whether extant liability rules, conceived for traditional vehicles, allow for an effective compensation mechanism based on the RMA, and how they influence the development and diffusion of CAD. Since a full automation, level 5 SAE CAD is not to be expected in the near future, the present analysis will consider high-level of automation solutions that still require the involvement of the driver.

### 5.5.2. Existing legal framework

Traffic liability rules *per se* are not set forth at EU level, but at MS' level. Since CAD could fall – in most cases – under the definition of vehicle, MS' legislation on traffic accidents and corresponding insurance requirements apply, when ad-hoc legislation is lacking.

At the EU level, mandatory insurance requirements are set forth by the Directive 2009/103/EC on the insurance against civil liability in respect of the use of motor vehicles (henceforth MID)[283], which imposes compulsory third-party liability insurance on the owner for damages to property, loss and personal injury inflicted on another party because of the actions of the policyholder (art. 9 MID). Such third-party insurance covers damages caused to pedestrians and all passengers, other than the driver (art. 12 MID). Furthermore, under art. 9, the MID sets minimum insurance coverages and under art. 18 victim's direct right of recourse for enforcing the insurance policy. Additionally, the MID obliges MS to set up victims' compensation funds for accidents caused by unidentified or uninsured vehicles, as well as for accident caused by a third-country vehicle (art. 7 to art. 11 MID)[284].

[279] E.g.: driving advanced systems (ADASs), automated vehicles (AVs), connected and automated vehicles (CAD), connected, cooperative and automated mobility (CCAMs).

[280] The levels of automation are classified differently throughout the world. The most famous classification is that set by SAE International (SAE J 3016). On this spectrum and for the purpose of this study, ADASs that merely facilitate or increase the safety of driving and support the driver through features such as night vision and GPS navigation, are not deemed as an ADS, but merely as a preliminary step towards the implementation of CAD and CCAMs.

[281] Evas. See esp., 50.

[282] SAE (2018). J3016_201806 - Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles. https://www.sae.org/standards/content/j3016_201806/, Society of Automotive Engineers. (last accessed June 29th 2020).

[283] Directive 2009/103/EC of the European Parliament and of the Council of 16 September 2009 relating to insurance of civil liability in respect of the use of motor vehicles, and the enforcement of the obligation to insure against such liability (OJ L 263, 7 October 2009, 11-31). The definitions of vehicles provided under art. 3 n.9 of the FD and art. 1 n. 1 of the MID are able to accommodate CAD under their scope of application as neither of them imply that a vehicle is such only if driven by a human driver.

[284] The MID was subject to the EC's REFIT evaluation which resulted in an amendment proposal of the MID. Under the latter, no amendments are suggested regarding insurance of CAD, as ADS fall within the scope of the MID and are adequately regulated therein. Thus, the victim's right to compensation is ensured by the owner's compulsory third-party liability insurance policy, which may in turn file a claim against the manufacturer. Information about the REFIT of the MID can be found at the following link https://ec.europa.eu/info/consultations/finance-2017-motor-insurance_en.

As for MS traffic liability and insurance regime, a recent comprehensive study for the European Parliament[285], showed a significant varied scenario: «(i) in some MS, specific legislation has been adopted for CAD (UK and Germany), while in other no such initiatives have been undertaken yet; hence, should an accident involving CAD occur, traditional traffic liability rules would apply (Italy, France, Spain, Sweden, the Netherlands, Austria); (ii) across MS, different forms of liability apply, ranging from fault-based liability, to strict and objective liability, to a combination of the two»[286].

Germany and the UK have enacted ad-hoc legislation for CAD liability. Under German provisions enacted in 2017[287], the behaviour of the driver of a high or fully automated vehicle up to level 4 SAE is regulated and specific duties are imposed on the latter, such as a duty to supervise the driving task, and resume control when indicated by the system, or when objective circumstances require him to do so. The failure to comply with said duties attracts driver's fault-based liability. Absent driver's fault, the owner shall be liable under the enacted legislation. Said legislation also imposes certain duties regarding the registration, transmission and deletion of data recorded by the CAD and required to prove whether the driver complied with its statutory duties, although only at a general level, as the specific holders of the duties and procedures shall be further set forth by the Federal Ministry for Transport and Digital Infrastructure, in consultation with the Data Protection and Information Protection Officer[288].

The 2018 Automated and Electric Vehicle Bill enacted in the UK[289] provides for a compulsory insurance covering the technical failures of the CAD technology and it provides for both first-party and third-party insurance. If the CAD is not insured, the owner will be liable. Further, the liability framework set forth therein is semi fault-based, as it burdens the owner of the vehicle with a duty to install safety-critical updates. Failure to comply with said duties, provided the failure caused the accident, will result in a denial of compensation to the owner, and it also allows insurance companies to act in recourse.

If this is the applicable framework as far as traffic liability is concerned, CAD – both as final product and in their components – may qualify as product under the PLD, and thus trigger the application of the PLD in case of defective functioning.

Indeed, when damages are caused by a defective CAD, the claimant may have to sue one or several parties that contributed in the production line, such as the software provider, hardware provider, the infrastructure provider, etc., and when the producer cannot be identified, the importer and the seller of the product, for defects in the CAD.

[285] Evas, T. (2018). A common EU approach to liability rules and insurance for connected and autonomous vehicles. European Added Value Assessment Accompanying the European Parliament's legislative own-initiative report (Rapporteur: Mady Delvaux), EPRS European Parliamentary Research Service.

[286] See in this respect Timan, T., R. Snijders, M. Kirova, S. Suardi, M. v. Lieshout, M. Chen, P. Costenco, E. Palmerini, A. Bertolini, A. Tejada, S. v. Montfort, M. Bolchi, S. Alberti, R. Brouwer, K. Karanilokova, F. Episcopo and S. Jansen (2019). Study on safety of non-embedded software. Service, data access, and legal issues of advanced robots, autonomous, connected, and AI-based vehicles and systems: final study report regarding CAD/CCAM and industrial robots. Brussel, European Commission., Annex 3136 -139 and Evas, T. (2018). A common EU approach to liability rules and insurance for connected and autonomous vehicles. European Added Value Assessment Accompanying the European Parliament's legislative own-initiative report (Rapporteur: Mady Delvaux), EPRS European Parliamentary Research Service.

[287] BGBl. I pg. 1607, also available at https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl216s1306.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl216s1306.pdf%27%5D__1516706616435, (last accessed June 29th 2020).

[288] For a more detailed analysis see Timan, T., R. Snijders, M. Kirova, S. Suardi, M. v. Lieshout, M. Chen, P. Costenco, E. Palmerini, A. Bertolini, A. Tejada, S. v. Montfort, M. Bolchi, S. Alberti, R. Brouwer, K. Karanilokova, F. Episcopo and S. Jansen (2019). Study on safety of non-embedded software. Service, data access, and legal issues of advanced robots, autonomous, connected, and AI-based vehicles and systems: final study report regarding CAD/CCAM and industrial robots. Brussel, European Commission., Annex 3139-140.

[289] Automated and Electric Vehicles Bill 2018, available at www.legislation.gov.uk/ukpga/2018/18/enacted (last accessed June 29th 2020).

### 5.5.3. Assessment and recommendations

The above shows that in many cases, different bodies of law may overlap – the PLD and traffic liability – in case of accidents caused by ADS up to level 4 SAE that still allow, at least partially, for user's control of the driving task. Thus, imposing duties to insure is insufficient, so long as it is not clarified which party bears what risk, and who is to be held liable for each kind of accident.

The high number of potentially responsible parties, the strong interplay of the CAD components and the high level of technicality required to analyses information data and technical evidence submitted by the defendant, exacerbate the PLD criticalities. Thus, proving the causal nexus in such a scenario will most likely become disproportionately burdensome. As a consequence, litigation costs and time increase, thus hindering an effective access to justice. Furthermore, even if the attribution of liability and the causal nexus can be determined, producer's diverse defenses under art. 7 of the PLD substantially reduce a victim's incentive (in this case, most likely, the owner of the CAD) to claim damages based on the PLD.

Moreover, the PLD is being applied and interpreted differently across MS and regime differences are present, such as different liability caps of different scopes of application[290].

As indicated by existing case law in other jurisdiction (US and China)[291], access to data and its evaluation are critical for establishing whom, between the driver who and the producer, should be held responsible.

The duty to record data (through a black box, i.e. logging) and make it available to the victim is relevant, but insufficient (see Ch. 4, § 4.6.5 above). Such information is in fact difficult and costly to interpret for most claimants.

These issues can be managed through three alternative possible options, namely: (i) no action; (ii) reform of the PLD; (iii) adopting ad-hoc legislation.

The first option of based on no legislative initiative is not advisable as it will lead to the adoption by MS of CAD-specific legislation at national level, as it is the case in the UK and Germany, leading to undesirable legal and market fragmentation.

Reforming the PLD is only a sub-optimal solution for at least three reasons: (i) given its broad scope of application, its reform will be a complex and lengthy process, and by the time it is completed, the first option may already have prevailed; (ii) the issues arising from differences in its implementation and interpretation by the MS will persist; (iii) regulating CAD indirectly may complicate market penetration.

For these reasons, the adoption of ad-hoc legislation at European level, setting uniform rules, is to be preferred. This legislation should favor a RMA by burdening the party who is best positioned to insure and minimize risks and ensure compliance with safety-relevant duties (e.g.: update the vehicle's software). This would most likely be either the producer or the owner. A choice between the two should be made. Holding one or the other primarily liable would not necessarily effect who bears the economic consequences of the accident. Indeed, if the producer were to be deemed liable towards the victim, he could insure against such risks and transfer the cost onto the users through product's price. Yet, opting for one or the other of the possible alternatives could reflect upon the kind of technology that ultimately prevails (no human driver, or driverless as an option).

[290] See in this respect Timan, T., R. Snijders, M. Kirova, S. Suardi, M. v. Lieshout, M. Chen, P. Costenco, E. Palmerini, A. Bertolini, A. Tejada, S. v. Montfort, M. Bolchi, S. Alberti, R. Brouwer, K. Karanilokova, F. Episcopo and S. Jansen (2019). Study on safety of non-embedded software. Service, data access, and legal issues of advanced robots, autonomous, connected, and AI-based vehicles and systems: final study report regarding CAD/CCAM and industrial robots. Brussel, European Commission., Annex 3,132.

[291] Ibid., Annex 3, 142-144.

In any case, strict liability rules that clearly identify the responsible party are advisable, based on a one-stop-shop approach. Said solution would allow for a clear apportionment of liability and ease the access to justice of potential victims, while reducing litigation costs. Further, such a framework could also ease penetration of CADs in the market by avoiding technological fragmentation that may emerge if different liability rules are adopted at MS's level[292].

## 5.6. Medical robots and diagnostic-assistive technologies in medical care

### 5.6.1. Definition and relevant features

Advanced robotics and AI are already used, and are expected to be increasingly relied upon, in a variety of different medical settings, ranging from diagnosis and medical treatment, to surgery, with sector-specific applications, such as radiology or virology.

In the view of adopting a sectorial, bottom-up and functional regulation of AI, it is thus particularly important to address the challenges brought about by medical robots and AI. Indeed, similar applications substantially affect healthcare, because they are likely going to influence the behaviour of medical practitioners, possibly affecting the apportionment of liability, and leading to new frontiers of defensive medicine.

From a policy-making perspective, it is thus necessary to analyze how liability might be apportioned between (i) the medical practitioner, (ii) the manufacturer/programmer and (iii) the hospital/structure that decides to adopt the AI-based solution, and/or employs the practitioner, in light of existing rules, namely negligence and product liability. Such framework shall then be assessed on the basis of the incentives that it creates, making sure that it holds liable the party that is best positioned to manage risks, to propose possible reforms.

However, as clarified throughout the study, no one-size-fits-all approach may be adopted, even within a relatively narrow-tailored class of applications. Under the label «medical robots» or «medical AI», in fact, fall a broad variety of devices, which differ among one another for their technical features, diffusion, function and use.

A first distinction may be made between surgical robots, and a series of applications that may be referred to – in non-technical terms – as «intelligent assistants».

Surgical robots are complex robotic devices that allow doctors to perform surgery procedures with greater precision, flexibility and control than what is possible with conventional techniques, and in less invasive ways. A typical example of this is the Da Vinci Robot, a surgical system composed by a camera arm and a mechanical arm displaying a series of surgical instruments at its end, both of which are controlled by the surgeon, who sits at a console with a high-definition, magnified and 3-D view.[293] So far, this type of application has fallen out of the definition on AI-based technology, as it does not feature AI-related characteristics, such as the capacity to operate without human supervision. In this sense, studies have correctly highlighted how the Da Vinci robot – despite its innovative nature and disruptive application in medicine – is not, from a legal perspective, different from less advanced tools,

[292] Timan, T., R. Snijders, M. Kirova, S. Suardi, M. v. Lieshout, M. Chen, P. Costenco, E. Palmerini, A. Bertolini, A. Tejada, S. v. Montfort, M. Bolchi, S. Alberti, R. Brouwer, K. Karanilokova, F. Episcopo and S. Jansen (2019). Study on safety of non-embedded software. Service, data access, and legal issues of advanced robots, autonomous, connected, and AI-based vehicles and systems: final study report regarding CAD/CCAM and industrial robots. Brussel, European Commission., Annex 3,134.

[293] Intuitive Surgical Inc. https://www.intuitive.com/en-us/products-and-services/da-vinci#, (last accessed June 29th 2020). Palmerini, E., A. Bertolini, F. Battaglia, B.-J. Koops, A. Carnevale and P. Salvini (2016). "RoboLaw: Towards a European framework for robotics regulation." Robotics and Autonomous Systems 86: 78-85.

traditionally used by doctors[294]. However, companies have started working on AI-versions of said robots, which would be able to function autonomously, i.e. with limited human supervision, on the basis of data and instructions inserted by doctors themselves[295]. Thus, a perspective policy initiative on AI may need to take into account such developments. In particular, it would be necessary to assess whether current liability rules are fit to accommodate such system, and especially the problems connected to the human-robot interaction. Most likely, the strict liability of the producer, fashioned as to ensure a one-shop-stop, and risk-management based compensation, would offer the best solution

Under the a-technical label «intelligent assistants», on the contrary, we may find a variety of applications that are supposed to help medical practitioners in acquiring, analyzing and elaborating medical data.

One major example would be that of the medical expert systems. Generally speaking, an «expert system is a computer (consisting of hardware and software) that elaborates useful information, like a human expert, in a specific area. It can memorize, learn and communicate with other expert systems and with humans, assuming proper decisions and explaining why these decisions are assumed»[296]. In medicine, such devices use AI-based algorithms and complex data mining techniques to elaborate relevant medical information, together with the structured or unstructured data accessible to the system (patient, demographic, clinical and billing data), which they can then use to perform a series of functions: diagnosis, laboratory analysis, development of treatment protocols, teaching, etc.[297].

A particularly famous expert system is IMB's Watson, a question-answering computer system capable of answering queries posed in natural language[298], also used in the healthcare sector as a clinical decision support system. Indeed, the system allows physicians to pose questions describing symptoms and other relevant data, which Watson then elaborates, also on the basis of other available structured and non-structured information – such as the patient's medical and hereditary history, medical records, treatment guidelines, notes from healthcare providers, research studies, test and materials, as well as scholarly literature – and finally provides a list of possible diagnosis and recommendations. Despite Watson-like applications are still used mainly in research settings, their development for commercial use in the medical sector is increasing, and may soon require attention at the policy-making and legislative level[299].

Applications that resemble Watson's assistive-diagnosis capacities may have application in specific branches of healthcare, and in radiology in particular. Indeed, AI may be used for diagnostic and interventional radiology, for example through systems that help in the radiomics process (i.e. to extract a large number of quantitative features that the radiologist cannot assess based on intensity, shape,

---

[294] Leenes, R., E. Palmerini, B.-J. Koops, A. Bertolini, P. Salvini and F. Lucivero (2017). "Regulatory challenges of robotics: Some guidelines for addressing legal and ethical issues." Law Innovation and Technology 9: 1-44., 9.

[295] See for example the patent application for patent no. US9220570B2 for a system for performing an automated surgical procedure available at https://patents.google.com/patent/US9220570B2/en (last accessed June 29th 2020). The latter system is designed to operate under three modes of operation, namely: master-slave, semi-autonomous, and supervised autonomous. As stated in the application: (i) in master-slave mode, the surgeon directly controls the robot's motions to perform tasks, similar to the Da Vinci surgical robot, (ii) «in the semi-autonomous mode, the surgeon will provide the robot with action commands (e.g. place suture in specific location, cut tissue in a line, tie a knot) that the robot will perform using autonomously calculated trajectories and tool actuations»; and (iii) «in the supervised autonomous mode, the surgeon only provides the robot with an overall goal (e.g. perform anastomosis) and the autonomous program determines the actions necessary to complete the goal (e.g. location, number, tension, and order of sutures to place) without any input from the surgeon».

[296] Castillo, E., J. M. Gutierrez and A. S. Hadi, 2012, (2012). "Expert System and Probabilistic Network Models." 2-8.

[297] Vihinen, M. and C. Samarghitean, "Medical Expert Systems", Current Bioinformatics (2008) (2008). "Medical Expert Systems." Current Bioinformatics 56(3).

[298] Guthart GS and S. JK. (2000). The Intuitive telesurgery system: Overview and application. Proc 2000 ICRA Millenn Conf IEEE Int Conf Robot Autom Symp Proc. 1: 618-621.

[299] Koçak, B., Ö. Kılıçkesmez, E. Ateş and E. Ş. Durmaz (2019). "Radiomics with artificial intelligence: a practical guide for beginners." Diagnostic and Interventional Radiology 25(6): 485-495. Gillies, R. J., H. Hricak and P. E. Kinahan (2016). "Radiomics: Images Are More than Pictures, They Are Data." Radiology 278(2): 563-577, Sollini, M., L. Antunovic, A. Chiti and M. Kirienko (2019). "Towards clinical application of image mining: a systematic review on artificial intelligence and radiomics. ." European Journal of Nuclear Medicine and Molecular Imaging 46(13): 2656–2672..

size or volume, and texture)[300], and through computer assisted diagnosis[301] (i.e. helping the physician in terms of image acquisition and interpretation, e.g. in detecting, categorizing and identifying the stage of a lesion, and in monitoring it during the treatment)[302].

In this sense, both general expert systems and radiology computer assisted diagnosis tools pose particularly challenging issues for the regulation of medical AI, as they will play an increasingly important role in reaching an accurate diagnosis of the illness affecting the patient, as well as the ideal curing strategy. Indeed, based on recent research it is claimed that expert systems will reach an overall accuracy above 95% in their diagnostic capabilities, while maintaining that they will not replace medical practitioners in their role as doctors and care providers[303].

This puts such systems in a peculiar situation, since they are not meant to substitute the doctor, but only work as intelligent assistants: they formulate solutions of the kind «on the basis of data a, b, c, there is X% of probability of issue Y». Medical practitioners remain the only persons in charge, and thence liable, for the negative consequences suffered by the patient, at least *prima facie*[304].

Thence, when discussing liability for damages connected to the use of such systems, we should consider both the existing rules of product liability, as well as those related to medical malpractice. In fact, the expert system and computer assisted diagnostic tools work as a tool in the hands of a human agent, who may be held liable for a behaviour that was influenced, or should have been influenced, by the intelligent assistant.

In particular, a series of different scenario may occur. For the sake of simplicity, we will consider situations where the expert systems offer a diagnosis with a high percentage of expected correctness.

**Example 7**

> The medical practitioner uses an expert system that does not give the correct diagnosis, relies on it, and prescribes a treatment that turns out to be ineffective, or indeed harmful to the patient. This, in turn, could be due to: (a) a malfunctioning of the product, (b) an error in the elaboration of the relevant information, which falls within the ordinary error percentage (according to the producers' claim: 5%) of the system.

**Example 8**

> The medical practitioner does not use an available expert system, or does not conform to the diagnosis and treatment suggested by the latter, and the prescribed cure turns out be ineffective, or indeed harmful to the patient.

### 5.6.2. Existing legal framework

In the first scenario – the doctor conforms, the system was wrong – two different sets of liability rules may apply: product liability rules, holding the producer liable, and medical liability rules, burdening the

[300] Hosny, A., C. Parmar, J. Quackenbush, L. H. Schwartz and H. J. W. L. Aerts (2018). "Artificial intelligence in radiology." Nature reviews. Cancer 18(8): 500-510.

[301] ESR, European Society of Radiology (2019). "What the radiologist should know about artificial intelligence - an ESR white paper. ." Insights into imaging 10(1), Fujita, H. (2020). "AI-based computer-aided diagnosis (AI-CAD): the latest review to read first. ." Radiological physics and technology.

[302] Litjens, G., T. Kooi, B. E. Bejnordi, A. A. A. Setio, F. Ciompi, M. Ghafoorian, J. van der Laak, B. van Ginneken and C. I. Sánchez (2017). "A survey on deep learning in medical image analysis." Med Image Anal 42: 60-88. and Hosny, A., C. Parmar, J. Quackenbush, L. H. Schwartz and H. J. W. L. Aerts (2018). "Artificial intelligence in radiology." Nature reviews. Cancer 18(8): 500-510.

[303] See in this respect https://www.ibm.com/blogs/think/2017/03/training-watson-to-detect-melanomas-earlier-and-faster/ (last accessed June 29th 2020) and the research indicated therein – Z. Ge, R. Chakravorty, B. Bozorgtabar, A. Bowling, R. Garnavi, et al. "Exploiting Local and Generic Features for Accurate Skin Lesions Classification Using Clinical and Dermoscopy Imaging", to appear in the proceeding of The 2017 IEEE International Symposium on Biomedical Imaging.

[304] Ibid.

practitioner and/or the medical structure where the latter operated. In a typical case, the patient will sue the doctor and/or the hospital, for having followed instructions that proved wrong. If held liable, the latter may then sue the producer in recourse.

In the second scenario only medical law rules apply. Indeed, the patient will blame the doctor for having chosen not do something that might have prevented the damage, arguing that the diagnosis made by the expert system was correct, or because reliance on such system might have significantly increased the chances of reaching the most appropriate diagnosis, even if none of the two could actually be objectively demonstrated.

Thus, medical liability constitutes the first and most important legal framework for addressing the issue.

As comparative studies have highlighted[305], liability of medical practitioners is mostly regulated through the general principles of negligence, so that they will be held liable for the damage caused because of their malpractice if they have negligently violated the standard of medical care required from them[306]. In particular, the ascertainment of negligence is here conceived as a two-prongs test, whereby it is necessary to establish first whether even just one single man in the world possessed the knowledge that might have avoided the plaintiff suffering harm, and second determine whether such knowledge could have been demanded to the specific agent[307]. Whenever an expert system is used, the first prong of the test is majorly affected, as the possibility to rely on said system elevates the standard against which the single practitioner is to be measured.

In this sense, said systems actually resemble «best practices» and «medical guidelines», which are expressly recognized as demandable conduct by courts and even legislators across Europe.

In the UK, for example, the leading case *Bolam v Friern Hospital Management Committee* [1957] states that «A man is not guilty of negligence if he has acted in accordance with a practice accepted as proper by a responsible body of medical men skilled in this particular art». Indeed, despite no cases have yet been adjudicated on the liability of expert systems, the solution they elaborate may be considered analogous to a «responsible, reasonable and respectable opinion» constituting said best practices[308].

Likewise, under Italian law, no criminal liability is established in cases of simple negligence if doctor complied with guidelines and best practices (G&BP), compliance with G&BP influences the amount to be paid in compensation and – most importantly – both legal scholars and courts tend to treat compliance with G&BP as a *prima facie* case of diligence[309].

Indeed, the diagnosis made by diagnostic-assistive technologies may be deemed as constituting a more compelling ground for compliance than simple G&BP; the accuracy of the analysis is statistically assessed, the analysis is made with the only perspective of providing best care, and is specific to the

---

[305] Koch, B. A. (2011). Medical Liability in Europe: Comparative Analysis. Medical Liability in Europe. A Comparison of Selected Jurisdictions, De Gruyter 611.

[306] Ibid.

[307] Padovani, T. (2002). Diritto Penale. Milano, Giuffrè. 283.

[308] Bolam v Friern Hospital Management Committee [1957] 1 WLR 582. The requirements for a reasonable opinion are outlined in Bolitho v. City and Hackney Health Authority [1997] where it is stated that: «In the Bolam case itself, McNair J. stated [1957] 1 W.L.R. 583, 587, that the defendant had to have acted in accordance with the practice accepted as proper by a "responsible body of medical men." Later, at p. 588, he referred to "a standard of practice recognised as proper by a competent reasonable body of opinion." Again, in the passage which I have cited from Maynard's case, Lord Scarman refers to a "respectable" body of professional opinion. The use of these adjectives -responsible, reasonable and respectable--all show that the court has to be satisfied that the exponents of the body of opinion relied upon can demonstrate that such opinion has a logical basis. In particular in cases involving, as they so often do, the weighing of risks against benefits, the judge before accepting a body of opinion as being responsible, reasonable or respectable, will need to be satisfied that, in forming their views, the experts have directed their minds to the question of comparative risks and benefits and have reached a defensible conclusion on the matter».

[309] Legge 8 marzo 2017, n. 24, Disposizioni in materia di sicurezza delle cure e della persona assistita, nonche' in materia di responsabilita' professionale degli esercenti le professioni sanitarie. (17G00041) (GU n.64 del 17-3-2017 ).

patient. On the contrary, G&BP do not offer official record or certification mechanisms, might adopt a cost-minimizing perspective (not best interest of patient), and are not as narrow tailored.

As far as medical devices and medical tools are concerned, manufacturers are required to produce them and certify them according to the existing essential requirements (e.g. Medical Device Directive, and the Regulation superseding it[310]), and, whenever a damage derives from a defect or malfunctioning of the system, producers are responsible under the relevant liability regime in case of defect or malfunctioning, which, however, varies among different MS: the majority of MS consider medical devices falling both within the scope of the PLD, whereas Germany and, to a more limited extent, Spain, provide for particularly strict liability regimes that specifically apply to medicines[311].

Here, the general considerations made on the limited relevance and effectiveness of the PLD in § 3.4 above come into play.

Firstly, it is debatable whether diagnostic-assistive technologies indeed fall into the scope of application of the PLD as of today, for a twofold reason. Firstly, they normally operate as non-embedded software, which, as we have seen in § 3.4.1– is not clearly covered by the directive[312]. Furthermore, depending on the specific circumstances of the case, it may very well be that a doctor, for example, uses an expert system acquired by the hospital not as a product, but as a service, operating in the cloud. In this second case, again, its nature of digital service would lead the expert system outside the scope of protection granted by the PLD.

Even if the directive were to apply, however, significant problems would emerge as far as the assessment of the defective nature of the system is concerned. Most importantly, these problems would not only affect the procedural dimension – i.e. the evidentiary burden – but also the substantive dimension. Indeed, while it is undisputed that situation Example 7– malfunctioning systems – may trigger the application of the PLD (provided, again that they are considered as product), situation under Example 8 – percentage of error – would most likely fall outside the notion of defect, as a certain margin of error, especially if adequately disclosed, does not frustrate the level of safety and security that the user is entitled to expect from it.

Furthermore, it is debatable whether the malfunctioning or error in the system could be considered as having caused the damage, because – as we clarified above – the system is not responsible for the final decision, but merely provides an analysis which the doctor may rely upon. In this sense, if the doctor is considered to have relied on the system even if it would have been reasonable for her not to do so, producers may shield themselves from liability, by claiming that the doctor was responsible for the final choice. In this case, the doctor/hospital may sue the producer under contract law, claiming that the system does not perform as expected and thus there is a case of lack of conformity or breach, but most likely no redress may be sought under the product liability framework.

---

[310] Council Directive 93/42/EEC of 14 June 1993 concerning medical devices, in OJ L 169, of July 12th, 1993. Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Text with EEA relevance. ) OJ L 117, 5.5.2017, 1–175.

[311] See in this respect the Germany Medicinal Products Act (Arzneimittelgesetz – AMG) available at http://www.gesetze-im-internet.de/englisch_amg/englisch_amg.html#p0063 (last accessed June 29th 2020) and the Spanish Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias., available at https://www.boe.es/buscar/act.php?id=BOE-A-2007-20555 (last accessed June 29th 2020).

[312] Ernst&Young, Technopolis and VVA (2018). Evaluation of Council Directive 85/374/EEC on the approximation of laws, regulations and administrative provisions of the Member States concerning liability for defective products. Brussels, European Commission, 62. It shall be noted however that Regulation (EU) 2017/745 states in Recital 19 that: «it is necessary to clarify that 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. The qualification of software, either as a device or an accessory, is independent of the software's location or the type of interconnection between the software and a device».

### 5.6.3. Assessment and recommendations

Against this background, it seems likely that, under existing liability rules, medical practitioners will tend to adopt defensive medicine practices and decision making, i.e. recommending a diagnostic test or medical treatment that is not necessarily the best option for the patient, but that mainly serves the function to protect the physician against the possible subsequent claims for damages by the patient or his family.

This could happen both regarding the choice of using computer assisted diagnostic systems, as well as the decision to conform to the suggested diagnosis and treatment – in particular when requesting additional test –, because not doing so may lead to increased chances of being exposed to liability, especially in systems – like Italy –, where the doctor is primarily sued in cases of medical malpractice.

Likewise, this tendency may be complemented by a progressive de-responsabilization of the physician, who could use disclosure about her choice to conform or not to conform to the system's diagnosis as a way of shifting on the patient's informed consent the risk of adopting a specific curing strategy[313].

This scenario is highly undesirable. To counteract it, it may be appropriate to revise existing liability rules – or anyway limit their exposure – as to shield doctors from responsibility connected to the use of medical systems, and rather hold strictly and absolutely liable either the hospital, or the producer or provider of the medical assistive technology, eventually under a specific form of enterprise-liability.

## 5.7. Drones

Given their diffusion and increasing and novel use, drones[314] require an assessment with respect to the extant civil liability framework applicable thereto and a determination on whether, existing legal frameworks are sufficient from a RMA perspective or whether new rules and measures ought to be adopted[315].

To that end, this section will: (ii) analyze and assess liability rules applicable to drones and (iii) formulate recommendations (§ 5.7.2).

With respect to the first point of analysis, drones are regulated both at EU and MS' level. At EU level, the main body of law is comprised by Regulation 2018/1139 on common rules in the field

[313] Montgomery v. Lanarkshire Health Board [2015]; Office of Technology Assessment, U. S. C. (1994). Defensive medicine and medical malpractice. http://biotech.law.lsu.edu/policy/9405.pdf, Feess, E. (2012). "Malpractice liability, technology choice and negative defensive medicine." The European Journal of Health Economics 13(2): 157-167.

[314] The term «drone» is a-technical one used to refer either to «controlled manually by means of a remote controller requiring a highly skilled operator […] or precisely controlled from the remotely spaced programmable computers using the on-board autopilot and global positioning system (GPS)» - see in this respect Hasan, K. M., S. H. Shah Newaz and M. Shamim Ahsan (2018). "Design and development of an aircraft type portable drone for surveillance and disaster management." International Journal of Intelligent Unmanned Systems 6(3): 147-159. Further, both engineering and social science literature – including legal one – use many terms to refer to such kind of applications, such as Autonomous Aircraft (AA), Unmanned Aircraft (UA), Unmanned Aircraft Systems (UAS), Unmanned Aerial Vehicles (UAV), Small Unmanned Aircraft (SUA), Remotely Piloted Aerial Vehicle (RPAV), Remotely Piloted Aircraft Systems (RPAS). For the purpose of this analysis, both the word «drones» and its acronyms shall be used.

[315] Such a need has been expressed in numerous EU institutional documents: (i) In the European Commission (2014). Communication from the Commission to the European Parliament and the Council: A new era for aviation. Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner, COM (2014) 207 final, Bruxelles. http://eurlex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52014DC0207, the EC stated that «the progressive integration of RPAS into the airspace from 2016 onwards must be accompanied by adequate public debate on the development of measures which address societal concerns including safety […] third party liability and insurance»; (ii) in the European Parliament resolution, of 29 October 2015 on safe use of remotely piloted aircraft systems (RPAS), the European Parliament «considers the question of identifying drones, of whatever size, to be crucial; underlines that solutions should be found which take into account the recreational or commercial use to which drones are put»; (iii) Paragraphs 24 and 30 of the CLRR includes drones in the analysis of «Remotely piloted, automated, connected, and autonomous ways of road, rail, waterborne and air transport», and it identifies safety, security and privacy as the main issues, related to drones, that Union law needs to protect.

of civil aviation and establishing a European Union Aviation Safety Agency [316] (henceforth RCA) and the Insurance Regulation No 785/2004[317].

The RCA regulates the registration and certification applicable to drones and the general rules of conduct operators of said applications must abide by, leaving outside of its scope insurance and liability rules. The RCA resides on the notion of «unmanned aircraft» (UA) which is defined under art. 3 (30) RCA as any aircraft: «operating or designed to operate autonomously or to be piloted remotely without a pilot on board». By employing a risk-based and class-based approach, the RCA includes in its scope all unmanned aircraft, regardless of the weight or use[318], whether fully autonomously operated or piloted remotely, and it expressly excludes state-operated devices as per art. 2(3)(a), RCA.

The specific certification and registration requirements are set forth through implementing and delegated acts of the Commission as recalled by art. 57 and 58 RCA[319]. Both the RCA and the subsequent implementation acts rely a on risk-centered perspective, whereby specific applicable rules take into account the overall degree of danger UA may create – which is the main criteria for classification employed by the RCA – and the «the operation or type of operations» the device is to perform. Thus, the legislation takes the peculiar characteristics of each application into account, establishing three categories of UAS operations («open», «specific» and «certified») with different safety requirements, proportionate to the risk they might give rise to. Further, in order to foster the identification of the responsible parties, the RCA provides for uniform registration requirements and systems, to be accessible to all MS, while the implementing act require new drones to be individually identifiable, allowing the authorities to trace a particular drone if necessary.

On the contrary, insurance requirements for aircraft operators and air carriers are set forth under the Insurance Regulation No 785/2004. The latter does not, however, provide any definition of drone and adopts a mass-based classification applicable to all aircrafts. Thus, drones are subject to said insurance requirements as long as they fall under the general definitions provided under the Insurance Regulation No 785/2004[320].

As opposed to the RCA, MS provide different definitions for UA which show some degree of variation[321], sometimes including and other times excluding autonomously operated aircraft, and generally classify them according to their weight. For example, Swedish legislation encompasses both remotely piloted aircraft and autonomously operated ones[322], while the Netherlands, prohibits the latter category

[316] Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91, in OJ L 212/1 of 22.8.2018..

[317] Regulation (EC) No 785/2004 of the European Parliament and of the Council of 21 April 2004 on insurance requirements for air carriers and aircraft operators, in OJ L 138, 30.4.2004, as amended by Commission Regulation (EU) No 285/2010 of 6 April 2010 amending Regulation (EC) No 785/2004 of the European Parliament and of the Council on insurance requirements for air carriers and aircraft operators, OJ L 87, 7.4.2010, 19–20.

[318] As per Recital 34 RCA, the notion of UA includes «model aircraft», defined as an unmanned aircraft «primarily used for leisure activities».

[319] Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft (Text with EEA relevance.), OJ L 152, 11.6.2019, 45–71, as amended by Commission Implementing Regulation (EU) 2020/639 of 12 May 2020 amending Implementing Regulation (EU) 2019/947 as regards standard scenarios for operations executed in or beyond the visual line of sight, OJ L 150, 13.5.2020, 1–31, Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems, OJ L 152, 11.6.2019, 1–40.

[320] See art. 3(a), Insurance Regulation No 785/2004 which defines air carrier as «an air transport undertaking with a valid operating licence». Under art. 3(c), Insurance Regulation No 785/2004, aircraft operator means «the person of entity, not being an air carrier, who has continual effective disposal of the use or operation of the aircraft».

[321] For a detailed analysis on MS adopted definitions and criteria of classification see Bertolini, A. (2018). Artificial Intelligence and civil law; liability rules for drones. Brussel, European Parliament.24-34

[322] See in this respect (UAS) TSFS 2009:88 AVIATION Series GEN.

radically[323], as opposed to the Czech Republic[324], which allows both, while keeping them separate. With respect to classification, most MS still resort to weight as the main criterion[325].

### 5.7.1. Existing legal framework

As mentioned above, the RCA does not directly address issues of liability and insurance. However, the RCA and the delegated and implementing regulations consider the operator responsible «for the operation» of the drone, as operators are required to ensure both the safety of the devices and of third-parties on the ground and of other airspace users, by abiding «the laws, regulations and procedures, pertinent to the performance of their duties, prescribed for the area, airspace, aerodromes or sites planned to be used […]». Said duties of care on operators are further formulated by the implementing regulations, which substantially extend them, and also provide detailed ones for drones' pilots in case of «specific» operations.

Furthermore, the Insurance Regulation No. 785/2004 imposes a unilateral compulsory insurance[326] on the operators of different air carriers and said insurance requirements differ based on a mass-based criterion. Two notable exceptions are provided, namely for model aircrafts with a maximum take-off mass (MTOM) of less than 20 kg, and aircrafts with a MTOM inferior to 500 kg – provided that they are not used for commercial purposes or are used for local flight instruction that does not require border crossing[327]. Said devices will thus be subject to insurance as and if provided for the MS' legislation, which may give rise to fragmentation issues with respect to redress mechanism applicable throughout the EU. More, devices with a MTOM inferior to 500 kg need to be insured for a minimum of 750.000 Special Drawing Rights. This choice may be criticized in light of the fact that the risk, the potential damage, the insurance coverage and the premium should be proportionate with or at least take into account other factors than the MTOM, such as the height of the area over which the UA is flying and the operator's experience.

On the other hand, legislation enacted at MS' level is articulated and includes detailed liability rules based on aviation rules[328]. The majority MS adopt at least one strict liability rule[329], burdening primarily the operator[330] and in other cases, the owner[331], or both[332]. Exceptionally, the pilot may be also held liable[333]. However, a few MS (i.e. Ireland and Czech Republic) as well as the UK enacted fault-based liability resting on standards of care, favoring, thus, the agent over the potential victim as opposed to strict liability rules, which instead, favor the claimant, by easing the burden of proof. Further, MS'

[323] See in this respect Article 1 of the Regulation of remotely – piloted aircraft systems of 6 October 2017 - Regeling op afstand bestuurde luchtvaartuigen Geldend van 01-07-2016 t/m 06-10-2017.

[324] See in this respect Act 49/1997 Coll. on civil aviation and amending Act 455/1991 Coll. on trade licensing (Trade Licensing Act) as amended by later regulations (further referred to as Civil Aviation Act).

[325] For a detailed analysis on MS adopted definitions and criteria of classification see Bertolini, A. (2018). Artificial Intelligence and civil law; liability rules for drones. Brussel, European Parliament. 24-34

[326] Said obligation is unilateral, as opposed to compulsory motor insurance, as insurers do not have an obligation to insure potential operators.

[327] Art. 2.2(g), Insurance Regulation No 785/2004.

[328] This is the Italian case where a relevant amount of regulation on UA is based on provisions enacted before the diffusion of drones.

[329] For a detailed overview see Bertolini, A. (2018). Artificial Intelligence and civil law; liability rules for drones. Brussel, European Parliament., 45-55.

[330] Such as Spain, France (which burdens the owner too) Belgium (which burdens the pilot as well), Italy (which holds the user liable, too) and Poland. Some more countries burden primarily the operator, too, but according to a fault-based approach.

[331] Such as Denmark, Sweden, the Netherlands, Austria and Germany, though in the two latter countries the owner is entitled to prove that the drone was being used against his will in order to be exempt from the duty to compensate for damages.

[332] This is the case for France (in case of leasing), Austria, and Germany.

[333] This is the case in Belgium. Italy and Denmark make reference to the «user» instead of the «pilot», but the two notions oftentimes overlap, especially if the device is remotely piloted and not totally automated, which is the case for the absolute majority of UA as of now.

liability rules in certain cases limit the overall exposure of the responsible party by providing liability caps[334].

With respect to insurance, as mentioned above, UAs that meet the criteria set forth in the Insurance Regulation No 785/2004 are subject to the compulsory insurance provided therein. Additionally, most MS set forth a duty to acquire third-party liability insurance for devices outside the scope of the Insurance Regulation No 785/2004[335], differentiating among MTOM classes and between commercial and non- commercial users[336]. The existing differences in insurance requirements for drones outside the scope of the Insurance Regulation No 785/2004 show that at EU level, at least for some types of devices and applications, fragmentation is present.

Furthermore, since drones are products for the purposes of art. 2, PLD, the European regime concerning the liability for defective products is applicable.

As already clarified (Ch. 3, § 3.4) under the PLD, the claimant seeking compensation «[…] shall be required to prove the damage, the defect and the causal relationship between defect and damage»[337]. Despite the claimant not being required to identify the specific cause of the defect, proving the defect and the causal relationship might still prove cumbersome, as it requires technical skills, special expertise and access to information which most likely the victim will not posses. These criticalities are very well applicable to drones as they display a high-degree of technological complexity. Moreover, a case involving a defective drone will often not be decided only based upon the PLD, but also on MS' tort and contract law, as the theoretical contribution of the human operating the device cannot be excluded *ab intio*.

### 5.7.2. Assessment and recommendations

Under a RMA, liability shall be attributed to the party that is best positioned to minimize risks and acquire insurance, thus decoupling *ex ante* deterrence – to be achieved via safety regulation – and *ex post* compensation.

Thus, as already regulated by some MS and as it may be deducted from the RCA and the implementing and delegated legislation, pursuant to a RMA the operator is the best party to manage the risks associated with the use of drones. Furthermore, in order to limit litigation costs and to foster an easy access to justice for the victim, liability should not be fault-based, but strict and objective and – given that damages and economic consequences arising from the use of drones will not, most likely and in principle, be catastrophic, liability caps are not required.

Under a RMA, criteria that increase the overall potential risk of the single application, might justify the imposition of specific requirements with respect to certification and also insurance. With respect to future EU liability rules, the risk-based approach justifies a variation granted on the purpose for which the drone is used (commercial or recreational) detailing the duties of care applicable to professional operators as opposed to operators for recreational use. However, the party bearing the responsibility

[334] Such as Austria and in Germany, where liability caps depend on the drone's MTOM. Under Italian law, the minimum insurance coverage is the same as the one provided under EU legislation, except for the case of operator's negligence when liability is unlimited. Similarly, Spain legislation provides where a liability cap of 220 000 SDR and liability is unlimited for gross negligence or intentional misconduct.

[335] For a detailed examination see Bertolini, A. (2018). Artificial Intelligence and civil law; liability rules for drones. Brussel, European Parliament., 46-55. Spain, France, the United Kingdom, Italy, Denmark, Sweden, and Germany enacted a general obligation to insure, while most other MS require insurance in the majority of hypotheses.

[336] Drones for non-commercial use (in Belgium) and toy-drones (in Austria) are allowed to be operated without insurance. Other MS differentiate based on weight and purpose: in the Czech Republic insurance is compulsory for all drones, apart from the ones that are both a) lighter than 20 kg, and b) commercially employed. In Poland, all drones weighing more than 5 kg must be insured, as well as lighter ones, when commercially employed. In the Netherlands, a minimum coverage of € 1 million is required for all drones commercially employed.

[337] Art. 4, PLD.

should remain the same and thus, from this perspective, the liability scheme should be identical regardless of the nature and size of the application.

Based on the above analysis of the RCA and MS' legal frameworks, extant legislation should be deemed adequate pursuant to a RMA in the majority of cases where the burden is on the party who may best identify and manage risks efficiently. Thus, liability rules should be strict and not fault-based. Moreover, based on a one-stop-shop approach, said rules should attribute liability to the operator of the device, as the latter is best positioned to manage risks associated with the use of drones, and acquire insurance. However, following the existing liability model of some of the MS, in the case of non-commercial use of drones, it is advisable to hold the owner responsible, as it might be easier to identify, either alone or jointly and severally with the operator. Additionally, when the damage derives from a defect of the device, the burdened parties might act in recourse against the producer under the PLD, thus leading to a fair apportionment of liability.

Nevertheless, when said liability rules overlap with other liability regimes, the effectiveness of the redress and compensation mechanism may be compromised. As discussed in Chapter §3, the criticalities of the PLD regarding informational asymmetry, the development risk defense and the victim's burden to prove the causal nexus between the damage and the defect of a widely used, albeit advanced technology, may prove burdensome, and limit the possibility of further apportionment of liability through secondary litigation.

Against this background, and in order to avoid fragmentation, the adoption of uniform EU rules is the most advisable option for regulating civil liability for the use of drones. Said uniformity shall be built upon the RCA model, which rightfully follows the risk-based approach and offers uniform certification and registration requirements applicable to a wide range of UAs, to avoid potential fragmentation deriving from diverging technical solutions. Moreover, the RCA employs the sound solution of making certification and registration requirements dependent on the general level of risks associated with the use of the aircraft.

Furthermore, the extant insurance legal framework, both at EU level and MS' level, provides for additional guarantees for victim's compensation. Nevertheless, the latter framework regulates insurance requirements, in principle, based on the MTOM. Thus, given the strong interplay between the RCA and the Insurance Regulation No 785/2004, coordination between the two should be sought in the sense that the latter could be amended so as to make its criteria mirror those the RCA adopts for certification purposes. Such an option is advisable, as the overall degree of risk employed by the RCA is relevant for insurance and may complement the MTOM, set forth by Reg. No 785/2004. The overall degree of risks assessed on elements such as the height of the area over which the UA is flying at and the operator's experience will and should most likely influence insurance coverage and premium, as well as the very duty to insure. Thus, exceptions may be provided for model aircraft and toy drones, as it is the case in certain MS, since – due to their specific purpose and use – they would bring about only limited risks.

Finally, although the aforementioned rules may offer redress in the majority of cases, a compensation fund may still be required as the effectiveness of the extant insurance mechanism may be weakened when the device is not insured, or not identified (e.g. when lost or wholly destroyed after the accident). Also, it may be that in certain cases the insurance cannot provide coverage, such as when the operation at matter is not duly approved or in the case of insurer's insolvency. More, implementing such a fund would be suitable, given the wide diffusion of drones (sustained by their facile use and inexpensiveness), as suggested by both a 2014 study funded by the European Commission[338], and a 2016 study funded by the European Parliament[339]. Such a fund could be financed by making insurers pay a part of the insurance premium they receive, as it's the case for funds for road accidents.

[338] Steer Davies Gleave (2014). Study on the Third-Party Liability and Insurance Requirements of Remotely Piloted Aircraft Systems, European Commission. See esp., 20 ff.

[339] Tomasello, F. and M. Ducci (2016). Research for TRAN Committee: Safe Integration of Drones into Airspace. Brussels, European Parliament. See esp. Section 4.9.3, 39.

# 6. POLICY RECOMMENDATIONS

The study discussed the notion of AI and AI-based technologies (Ch. 1), their qualification as products, and a functional notion of legal personhood (Ch. 2), and analysed the extant European product safety and liability framework (Ch. 3). It addressed current proposals developed at EU level – in particular the EG's report on AI liability published by the New Technology Formation – (Ch. 4), and proposed an innovative approach to the regulation of liability – i.e. the Risk Management Approach (RMA) – (Ch. 4-5). Finally, four case-studies were assessed pursuant to the RMA, to propose reform when needed (Ch. 5).

Against this background, the following policy recommendations may be formulated.

***Regulatory approaches. Need for legal certainty and legal protection to unlock technological innovation***

1. Policymakers and legislators should ensure that their legal systems are fit for accommodating new technologies, such as AI-based applications, which may bring great societal benefit [§ 4.1].
2. Such adequacy is reached when legal rules (i) are certain and incentivise the development, commercialization and use of new technologies, and do not lead to legal and market fragmentation, (ii) increase users' trust in the use and reliability of technologically advanced solutions and willingness to purchase more innovative goods [§ 4.7.6, §4.7.7].
3. Thus, technology regulation should: (i) occur at EU level to achieve maximum harmonization and consumer protection, possibly through regulations rather than directives; (ii) ensure fair distribution of the costs and benefit derived from technological-development; (ii) grant effective protection against the damage which may be caused therefrom [§ 4.1, § 4.2, § 4.7 & §4.7.6 - 4.7.7].
4. To this end, policy makers and legislators shall avoid technology neutral regulatory regimes, even with respect to civil liability rules. This approach is not technically feasible, nor desirable from a policy perspective [§ 4.7.1, § 4.7.2, § 4.7.7, § 5.2].
5. Indeed, there is no single notion of AI. Even from a technological perspective, AI is best understood by looking at specific solutions, aimed at serving a given purpose or functions in defined settings [§ 1.3, § 1.5, § 4.7.1, § 4.7.2].
6. AI is pervasive and will be used in diverse fields – such as consultancy, consumer products and services, mobility, online connectivity, energy production and distribution, police and justice administration –, where EU and MS liability rules are already sector-specific. The advent of AI does not justify a shift towards a universal regulatory approach [§ 4.7, § 4.7.1].
7. A class-of-application-by-class-of-application approach is required [§ 4.7.2, § 4.7.7, §§ 5.1-5.3].
8. Thus, AI-based solutions shall be clustered in sufficiently uniform classes of applications by identifying technologies presenting similar technical traits, as well as corresponding legal, social, and economic concerns [§ 4.7.2].
9. Only technologies that give rise to relevant risks and potential that are not well framed within the current legal system, should be specifically regulated. While normative intervention at EU level is of fundamental importance, it should be minimally invasive in all non-strictly relevant cases, according to the principle of proportionality and subsidiarity [§ 4.7.1, § 4.7.7].

### *Simplifying liability rules through a Risk Management Approach: prioritizing victim compensation to incentivize the uptake of advanced technologies*

10. Pursuant the considerations under n. 3 above, extant legal rules should be assessed and reformed, and new rules should be formulated, according to their adequacy to accommodate and incentivize desired technological development and, in particular, depending on their capacity to ensure legal certainty as well as effective legal protection [§ 4.7, § 4.7.1] .
11. To achieve said goals, a Risk-Management Approach (RMA) is needed [§ 4.7.2, § 4.7.7, §§ 5.1-5.3].
12. Under the RMA, liability shall be to strict – if not absolute –, rather than fault-based. Indeed, ex a*nte* safety should be decoupled from *ex post* compensation, leaving it to other and more effective mechanisms – such as safety-regulation – to incentive desired standards of conduct. To this end, product safety framework shall be further exploited by adopting *ex ante* detailed regulation and technical standards, to better accommodate emerging technologies [§§5.1-5.3].
13. To ensure prompt and full compensation, said strict or absolute liability shall be attributed to a single, clear and unquestionable entry point for all litigation (one-stop-shop) [§ 4.7.4, § 5.2].
14. The subject who is held liable should be identified *ex ante* as the party which is best positioned to (i) identify a risk, (ii) control and minimize it through its choices, and (iii) manage it, ideally pooling and distributing it among all other parties, eventually through insurance, and/or no-fault compensation funds [§§ 5.1-5.3].
15. This party will vary according to the classes of application considered, in light of their complexity and functioning, as well as the way incentives are shaped [§4.7.2, § 4.7.7, §§ 5.1-5.3].
16. The responsible party will not necessarily bear the economic costs of the accident. Through insurance and price mechanisms he might transfer the cost to all users of a given technology (pooling and spreading effect) [§§ 5.1-5.3, § 5.5.3].
17. The responsible party should be granted rights to sue in recourse the other agents who might have contributed to causing harm (secondary litigation) [§ 4.7.4].
18. Similarly, contractual agreements among possible responsible parties to distribute risks along the value chain should be favoured. This should not alter the one-stop-shop approach described *sub* 13 above [§ 4.7.4, § 4.7.7].
19. To ease management of higher risks, different approaches might be used – depending on the type of technology, the subjects involved, the relevant market, and the overall regulatory framework involved –, either alone or in combination with one another. These solutions include: (i) compulsory fist- or third-party insurance, when statistical data allow adequate risk-assessment, since, absent such conditions, a generalized duty to insure would have a chilling effect; (ii) automatic compensation funds, financed through ad-hoc taxes/fees imposed on the producers, and/or service providers, and/or users of product or service, or through public spending; (iii) damage caps and limitations, proportionate to the specific risks brought about [§ 5.2].
20. When multiple parties contribute to providing complex AI-based applications – and services in particular – and identifying the optimal entry point for litigation is difficult, prompt compensation may alternatively be reached by granting legal personality to the specific class of application, where all the parties involved would bear the cost of liability according to their share of interest [§ 5.2].

### *Proposed solutions*

21. When assessed for its capacity to ensure legal certainty and effective legal protection of the victim, the product liability framework is questionable. Indeed, the product liability directive (PLD) fails to

achieve high levels of harmonization among MS and does not ensure adequate compensation to the victims [§§ 3.3-3.4].

22. A reform of the product liability directive (PLD) that eases the position of the claimant is advisable, since the opacity and complexity of many AI-based applications make it difficult to apportion liability among multiple potential responsible parties and to ascertaining a clear causal nexus between a given conduct and the harm suffered by the victim will become, leading to «alternative causation» scenarios [§§ 3.5-3.6].

23. Yet, reforming the PLD is not sufficient to successfully address the regulation of AI-based technologies at EU level, since – despite its theoretically broad scope of application – the high cost and complexity of its litigation only incentivizes high-value claims. Smaller smaller-value claims where non-professional victims seek redress form damage suffered as a consequence of the failure of a complex product, possibly affecting the product itself – which are certainly going to increase with the diffusion of automation –, will not be sufficiently protected by the PLD [§ 4.3].

24. Thus, AI-based technologies need to be addresses through ad-hoc legislation [§ 4.3].

25. Indeed, only those technologies that truly pose societal concerns give rise to relevant risks, and represent a new potential that is not well framed within the current legal system, should be specifically regulated. While normative intervention in this field is of fundamental importance at EU level, it should not be generalized and should be minimally invasive in all non-strictly relevant cases, according to the principle of proportionality and subsidiarity [§ 4.4, § 4.7.1, § 4.7.7].

26. Once that a class of application worthy of regulatory attention has been identified, applicable EU and MS legislation shall be assessed, according to the incentives it gives rise to and the legal and market failures it may cause (prevent effective legal protection and costs-internalization, hamper innovation). When needed, legal reforms might be formulated [§ 4.6.9, § 5.3].

27. Which type of technology shall be addressed, and in which order, is a matter of priority, to be defined according to the actuality or proximity of technological development and market diffusion of the given technology, and the relevance of the social concerns or benefits associated with it [§ 4.7.1, § 4.7.2, 4.7.7, § 5.2, 5.5].

### *Case studies*

28. Extant regulation of industrial robots (IR) is fit for accommodating technological evolution, since victims benefit from prompt and adequate compensation, through workers' health and safety legislation, and the related national insurance system, while business-users may sue, directly or in regress, the other subjects of the production chain, on a contractual basis. The application of the PLD is residual and limited to claims between business-users and producers, and is thus not excessively problematic. Despite some inefficiency (such as the lack of and adequate insurance market), IR appear overall well-regulated – ensuring an easy point of access for all litigation by the victim –, and intervention in this field should not be prioritized [§ 5.4].

29. As for drones, the applicable legal framework is partly adequate because national laws tend to converge on holding the operator (or the owner) strictly liable for failing to ensure the safety of drones' operation, while EU and national law set third-parties compulsory insurance, differentiating on the basis of the mass and use of the devices. However, overlap with the PLD and other liability regimes may lead to possible uncertainties and alternative causation scenarios. A European regulatory intervention, even with respect to liability, is therefore advisable to achieve maximum harmonization among MS, yet it is not a pressing necessity [§ 5.7].

30. On the contrary, the liability framework for damages caused by connected and automated driving (CAD) is not adequate: (i) increasing automation causes the PLD and national traffic liability rules

to overlap; (iii) apportioning liability becomes problematic, and exacerbates the major criticalities that the PLD displays; (iii) imposing duties to insure is per se insufficient, since it is not clear which party bears what risk. Furthermore, MS are starting to regulate CADs autonomously, leading to undesirable legal and market fragmentation. Ad-hoc legislation should be urgently adopted at EU level, holding strictly liable the party that is best positioned to insure and minimize risks. Said party may be either the owner or manufacturer of the vehicle, with partially different effects on the technology that will prevail [§ 5.5].

31. As for medical diagnostic assistive technologies, the legal framework deriving from EU and national law is not adequate and should urgently be revised, as it: (i) sees an overlap of product liability legislation and national provisions on medical malpractices, which are either contractual or tortious, and hold primarily the doctor liable in case of professional negligence; (ii) leads to defensive medical decision making. Existing liability rules should be revised as to shield doctors from responsibility connected to the use of medical systems or minimize their direct exposure. Hospital or producers should instead be held primarily liable through strict liability rules, or by establishing a form of enterprise-liability for service providers [§5.6].

# REFERENCES


- Committee on Legal Affairs (2020). Draft Report with recommendations to the Commission on a Civil liability regime for artificial intelligence (2020/2014(INL)), Brussel: European Parliament.
- Agre, E. P. (1997). Toward a Critical Technical Practice: Lessons Learned in Trying to Reform AI. Social Science, Technical Systems, and Cooperative Work: Beyond the Great Divide, G. Bowker, L. Gasser, L. Star and B. Turner. Erlbaum, Psychology Press: 496.
- AI HLEG (2019). A definition of AI: main capabilities and disciplines, European Commission., available at https://ec.europa.eu/digital-single-market/en/news/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines
- Albus., J. S. (1991). "Outline for a theory of intelligence." EEE Trans. Systems, Man and Cybernetics 21(3): 473–509.
- Anderson, J. M., P. Heaton and S. J. Carroll (2010). The U.S. Experience with No-Fault Automobile Insurance. A retrospective. Santa Monica (CA), Rand.
- Article 29 Data Protection Working Party (2018). Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 .
- Bayern, S. J. (2015). "The Implications of Modern Business-Entity Law for the Regulation of Autonomous Systems." 19 Stanford Technology Law Review 93.
- Beck, S. (2014). Corporate Criminal Liability. The Oxford Handbook of Criminal Law.
- Bertolini, A. (2013). "Robots as Products: The Case for a Realistic Analysis of Robotic Applications and Liability Rules." Law Innovation and Technology 5(2): 214.
- Bertolini, A. (2014). Robots and liability - Justifying a change in perspective. Rethinking Responsibility in Science and Technology. F. Battaglia, J. Nida-Rümelin and N. Mukerji. Pisa, Pisa University Press: 143-166.
- Bertolini, A. (2015). "Robotic prostheses as products enhancing the rights of people with disabilities. Reconsidering the structure of liability rules." International Review of Law, Computers & Technology 29(2-3): 116-136.
- Bertolini, A. (2016). "Insurance and Risk Management for Robotic Devices: Identifying the Problems." Global Jurist (2): 1-24.
- Bertolini, A. (2018). "Human-Robot Interaction and Deception." Osservatorio del diritto civile e commerciale, Rivista semestrale (2): 645-659.
- Bertolini, A. (2018). Artificial Intelligence and civil law; liability rules for drones. Brussel, European Parliament.
- Bertolini, A. and M. Riccaboni (2020). The Regulation of Connected and Automated Driving. A Law and Economics Analysis of Liability Rules. W. Paper.
- Bertolini, A. and Palmerini. E. (2014). Regulating Robotics: a Challenge for Europe. Upcoming Issues of EU Law, available at http://www.europarl.europa.eu/document/activities/cont/201409/20140924ATT89662/20140924ATT89662EN.pdf. D.-G. f. I. Policies. Bruxelles.
- Board, D. I. (2019). AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense. US, Department of Defense.

- Bonsignorio, F., E. Messina and A. P. del Pobil (2014). "Fostering Progress in Performance Evaluation and Benchmarking of Robotic and Automation Systems." IEEE Robotics & Automation Magazine (3): 22.
- Borghetti, J. S. (2016). Product Liability in France. European Product Liability. An Analysis of the State of the Art in the Era of New Technologies. P. Machnikowski. Cambridge, Intersentia: 205-236.
- Bryson, J. J. and P. P. Kime (2011). Just an artefact: why machines are perceived as moral agents. Proceedings of the Twenty-Second International Joint Conference on Artificial Intelligence: Barcelona, Catalonia, Spain, 16–22 July 2011. T. Walsh. Menlo Park, CA, USA AAAI Press. II: 1641-1646.
- Calo, R. (2011). "Open Robotics." Maryland Law Rev. 70.
- Castillo, E., J. M. Gutierrez and A. S. Hadi, 2012, (2012). "Expert System and Probabilistic Network Models." 2-8.
- Castronovo, C. (2006). "Diritto privato generale e diritti secondi la ripresa di un tema." Europa e diritto privato (2): 397-423
- Centre of European Contract Law (2000-2003). Principles of European Contract Law O. Lando. The Hauge, Kluwer Law International.
- Cianci, A. (2015). La nozione di responsabilità genitoriale. La riforma della filiazione. C. M. Bianca. Padova, Cedam. 579-595
- Coase, R.H. (1937), The Nature of the Firm. Economica, 4: 386-405.
- Commission of the European Communities (1999). Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions, Principles and guidelines for the Community's audiovisual policy in the digital age COM (1999) 0657 final. Brussels.
- Commission of the European Communities (1999). Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, Towards a new Framework for Electronic Communications Infrastructure and Associated Services: the 1999 Communications Review COM (1999) 539 final. Brussels.
- National Science and Technology Council Committee (2016). Preparing for the future of Artificial Intelligence. United States US Government, Office of Science and Technology Policy
- Council of Europe (1990), Recommendation No. R (88) 18 adopted by the Committee of Ministers of the Council of Europe on 20 October 1988 and explanatory memorandum, Liability of enterprises for offences. Strasbourg.
- Cuocci, V. V. (2013). Dall'assicurazione obbligatoria R.C. Auto alla no-fault insurance. Uno studio comparativo dei sistemi di traffic accident compensation. Milano, Giuffrè.
- Dachs, B. (2018). The impact of new technologies on the labour market and the social economy Brussels, STOA.
- Danish Government (2019). National Strategy for Artificial Intelligence. B. a. F. A. Ministry of Finance and Ministry of Industry. Rosendahls.
- Davies, R. (2015). Industry 4.0 Digitalisation for productivity and growth, European Parliament.
- Dawson, D., Schleiger E., J. Horton, J. McLaughlin, C. Robinson, G. Quezada, J. Scowcroft and S. Hajkowicz (2019). Artificial Intelligence, Australia's Ethics Framework. A Discussion Paper. Australia: 14.
- De Cristofaro, G. (2014). "Dalla potestà alla responsabilità genitoriale: profili problematici di una innovazione discutibile." Nuove Leggi Civili Commentate.

- Ernst&Young (2019). Report of Estonia's AI Taskforce Ministry of Economic Affairs, Government Office.
- Ernst&Young, Technopolis and VVA (2018). Evaluation of Council Directive 85/374/EEC on the approximation of laws, regulations and administrative provisions of the Member States concerning liability for defective products. Brussels, European Commission.
- ESR, European Society of Radiology. (2019). "What the radiologist should know about artificial intelligence - an ESR white paper." Insights into imaging 10(1).
- European Commission (2016). The 'Blue Guide' on the implementation of EU products rules 2016. OJ C 272, 26.7.2016. 1–149.
- European Commission (2017). SWD(2017)350. Commission Staff Working Document. Better Regulation Guidelines. Brussels.
- European Commission (2018). Commission communication of 25 April 2018 on Artificial Intelligence for Europe COM(2018) 237 final. Brussels.
- European Commission (2018). Commission Staff Working Document Evaluation of Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products SWD(2018) 157 final. Brussels
- European Commission (2018). Commission Staff Working Document. Evaluation of Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products. Brussels.
- European Commission (2018). Report from The Commission to The European Parliament, the Council and the European Economic and Social Committee on the Application of the Council Directive on the approximation of the laws, regulations, and administrative provisions of the Member States concerning liability for defective products (85/374/EEC). Brussels.
- European Commission (2020). Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics COM(2020) 64 final. Brussels.
- European Commission (2020). White Paper On Artificial Intelligence. A European approach to excellence and trust COM(2020) 65 final. Brussels.
- European Commission. (2020). Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee. Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics. Brussels.
- European Economic and Social Committee. (2017). Opinion of the European Economic and Social Committee on 'Artificial intelligence - The consequences of artificial intelligence on the (digital) single market, production, consumption, employment and society' (own-initiative opinion), OJ C 288, 31.8.2017, 1.
- European Group on Tort Law (2006). Principles of European Tort Law. Text and commentary. Vienna, Springer.
- European Parliament (2019). European Parliament resolution of 12 February 2019 on a comprehensive European industrial policy on artificial intelligence and robotics (2018/2088(INI)), Brussels.
- Evas, T. (2018). A common EU approach to liability rules and insurance for connected and autonomous vehicles. European Added Value Assessment Accompanying the European Parliament's legislative own-initiative report (Rapporteur: Mady Delvaux). Brussels: EPRS European Parliamentary Research Service.

- Expert Group on Liability and New Technologies – New Technologies Formation (2019). Report on Liability for Artificial Intelligence and other emerging digital technologies. Available at https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608
- Feess, E. (2012). "Malpractice liability, technology choice and negative defensive medicine." The European Journal of Health Economics 13(2): 157-167.
- Feldthusen, B. (2002). "Posturing, tinkering and reforming the law of negligence – a Canadian perspective." University of New South Wales Law Journal Forum 8(2).
- Floridi, L. (1999). Philosophy and Computing: an Introduction, Routledge.
- Floridi, L. and J. W. Sanders (2004). "On the Morality of Artificial Agents." Minds and Machine 14: 349–379.
- Foerste, U. and F. Graf von Westphalen (2012). Produkthaftungshandbuch. München, C.H. Beck.
- Fogel, D. B. (1995). "Review of computational intelligence: Imitating life." Proc. of the IEEE 83(11).
- Fujita, H. (2020). "AI-based computer-aided diagnosis (AI-CAD): the latest review to read first. ." Radiological physics and technology.
- Geistfeld, M. A. (2011). Principles of Products Liability. New York, Foundation Press.
- Germany, F. G. (2018). Artificial Intelligence Strategy: 4-5.
- Gillies, R. J., H. Hricak and P. E. Kinahan (2016). "Radiomics: Images Are More than Pictures, They Are Data." Radiology 278(2): 563-577.
- Government, F. (2017). Finland's Age of Artificial Intelligence Ministry of Economic Affairs and Employment
- Government, H. (2017). Industrial Strategy. Building a Britain fit for the future. UK: 37.
- Government, J. (2019). AI Strategy 2019 AI for Everyone: People, Industries, Regions and Governments (tentative translation）. T. a. I. Council for Science. Japan: 2-3.
- Greenberg, B. A. (2016). "Rethinking Technology Neutrality." Minnesota Law Review 100:1495.
- Grossman, P. Z., R. W. Cearley and D. H. Cole (2016). "Uncertainty, insurance and the Learned Hand formula." Law, Probability and Risk 5(1): 1-18.
- Guthart GS and Salisbury JK. (2000). The Intuitive telesurgery system: Overview and application. Proc 2000 ICRA Millenn Conf IEEE Int Conf Robot Autom Symp Proc. 1: 618-621.
- Gutman, M., B. Rathgeber and T. Syed (2012). Action and Autonomy: A hidden Dilemma in Artificial Autonomous Systems. Robo- and Informationethics. Some Fundamentals. M. Decker and M. Gutman, Lit Verlag: 231-256.
- Hasan, K. M., S. H. Shah Newaz and M. Shamim Ahsan (2018). "Design and development of an aircraft type portable drone for surveillance and disaster management." International Journal of Intelligent Unmanned Systems 6(3): 147-159.
- Helland, E. A. and A. Tabarrok (2012). "Product Liability and Moral Hazard: Evidence from General Aviation." The Journal of Law and Economics 55: 593.
- Horst, J. (2002). A native intelligence metric for artificial systems. In Performance Metrics for Intelligent Systems Workshop. Gaithersburg, MD, USA.
- Hosny, A., C. Parmar, J. Quackenbush, L. H. Schwartz and H. J. W. L. Aerts (2018). "Artificial intelligence in radiology." Nature reviews. Cancer 18(8): 500-510.
- Kalra, N. and S. M. Paddock (2016). Driving to Safety. How Many Miles of Driving Would It Take to Demonstrate Autonomous Vehicle Reliability?, Rand. Transportation Research Part A: Policy and Practice, 2016, vol. 94, issue C, 182-193 .

- Koçak, B., Ö. Kılıçkesmez, E. Ateş and E. Ş. Durmaz (2019). "Radiomics with artificial intelligence: a practical guide for beginners." Diagnostic and Interventional Radiology 25(6): 485-495.
- Koch, B. A. (2011). Medical Liability in Europe: Comparative Analysis. Medical Liability in Europe. A Comparison of Selected Jurisdictions, De Gruyter 611.
- Koops, B.-J. (2006). Should ICT Regulation Be Technology-Neutral?. STARTING POINTS FOR ICT REGULATION. DECONSTRUCTING PREVALENT POLICY ONE-LINERS. IT & LAW SERIES, Bert-Jaap Koops, Miriam Lips, Corien Prins & Maurice Schellekens, eds. The Hague, T.M.C. Asser Press. 9: 77-108.
- Koops, B.-J., Hildebrandt-Mireille and D.-O. Jaquet-Chiffelle (2010). "Bridging the Accountability Gap: Rights for New Entities in the Information Society?" Minnesota Journal of Law, Science & Technology 11(2): 497.
- Koziol and Wilcox (2009). "Punitive Damages: Common Law and Civil Law Prospectives." Tort and Insurance Law 25 (Institute for European Tort Law of the Austrian Academy of Science).
- Kraakman, R., P. Devies, H. Hansmann, G. Hertig, K. Hopt, H. Kanda and E. Rock (2006). The Anatomy of Corporate Law: A Comparative and Functional Approach.
- Krafft, P. M., M. Young, M. Katell, K. Huang and G. Bugingo (2019). Defining AI in Policy versus Practice. Proceedings of the 2020 AAAI/ACM Conference on AI, Ethics, and Society (AIES). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431304, SSRN.
- Kritikos, M. (2016). Legal and ethical reflections concerning robotics, STOA Policy Briefing. June 2016-PE 563.501, available at https://www.europarl.europa.eu/RegData/etudes/STUD/2016/563501/EPRS_STU(2016)563501(ANN)_EN.pdf
- Kurzweil, R. (2000). The age of spiritual machines: When computers exceed human intelligence, Penguin.
- Leenes, R., E. Palmerini, B.-J. Koops, A. Bertolini, P. Salvini and F. Lucivero (2017). "Regulatory Challenges of Robotics: Some Guidelines for Addressing Legal and Ethical Issues." Law Innovation and Technology: 1-44.
- Leenes, R., E. Palmerini, B.-J. Koops, A. Bertolini, P. Salvini and F. Lucivero (2017). "Regulatory challenges of robotics: Some guidelines for addressing legal and ethical issues." Law Innovation and Technology 9: 1-44.
- Litjens, G., T. Kooi, B. E. Bejnordi, A. A. A. Setio, F. Ciompi, M. Ghafoorian, J. van der Laak, B. van Ginneken and C. I. Sánchez (2017). "A survey on deep learning in medical image analysis." Med Image Anal 42: 60-88.
- M. A. o. Singapore (2019). Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Singapore: 5.
- Machnikowski, P. (2016). European Product Liability. An Analysis of the State of the Art in the Era of New Technologies. Cambridge, Intersentia.
- Magnus, U. (2016). Product Liability in Germany. European Product Liability. An Analysis of the State of the Art in the Era of New Technologies. P. Machnikowski. Cambridge, Intersentia: 237-274.
- Matthias, A. (2010). Automaten als Träger von Rechten, Logos Verlag.
- Maxwell, W. J. and M. Bourreau (2015). "Technology neutrality in Internet, telecoms and data protection regulation." Computer and Telecommunications L. Rev. 21(1), 1–4 (2015)
- McCarthy, J. (2007). What is Artificial Intelligence? http://www-formal.stanford.edu/jmc/whatisai.pdf.

- Ministerio de Ciencia, Innovación y Universidades (2019 ). Estrategia Española De I+D+I En Inteligencia Artificial I. y. U. Ministerio de Ciencia: 12.
- Navarretta, E. (2009). L'ingiustizia del danno e i problemi di confine tra responsabilità contrattuale ed extracontrattuale. Diritto civile. N. Lipari and P. Rescigno. Milan, Giuffrè. III, IV: 233-253.
- Nilsson, N. (2010). The quest for artificial intelligence. A history of ideas and achievements, Cambridge University Press.
- NITI Aayog (2018). National Strategy for Artificial Intelligence, India: 12.
- OECD (2011). Council Recommendation on Principles for Internet Policy Making, available at http://www.oecd.org/internet/ieconomy/49258588.pdf
- OECD (2017). The Next Production Revolution., available at http://www.oecd.org/publications/the-next-production-revolution-9789264271036-en.htm
- OECD (2019). Recommendation of the Council on Artificial Intelligence, OECD. LEGAL/0449., available at http://www.oecd.org/going-digital/ai/principles/
- Office of Technology Assessment, U. S. C. (1994). Defensive medicine and medical malpractice., available http://biotech.law.lsu.edu/policy/9405.pdf.
- Padovani, T. (2002). Diritto Penale. Milano, Giuffrè.
- Palmerini, E. and A. Bertolini (2016). Liability and Risk Management in Robotics. Digital Revolution: Challenges for Contract Law in Practice. R. Schulze and D. Staudenmayer. Baden-Baden, Nomos: 225-259.
- Palmerini, E., A. Bertolini, F. Battaglia, B.-J. Koops, A. Carnevale and P. Salvini (2016). "RoboLaw: Towards a European framework for robotics regulation." Robotics and Autonomous Systems 86: 78-85.
- Palmerini, E., F. Azzarri, F. Battaglia, A. Bertolini, A. Carnevale, J. Carpaneto, F. Cavallo, A. Di Carlo, M. Cempini, M. Controzzi, B.-J. Koops, F. Lucivero, N. Mukerji, L. Nocco, A. Pirni, H. Shah, P. Salvini, M. Schellekens and K. Warwick (2014). Guidelines on Regulating Robotics. Robolaw Grant Agreement Number: 289092, D6.2.
- Parliament, E. (2017). European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL).
- Polinsky, M. A. and S. Shavell (2009-2010). "The uneasy case for product liability." Harvard Law Review 123: 1437.
- Poole, D., A. Mackworth and R. Goebel (1998). Computational Intelligence: A logical approach. New York, NY, USA, Oxford University Press.
- Posner, R. (2007). Economic Analysis of Law, Wolters Kluwer.
- Puorro, A. P. (2013). "High Frequency Trading: una panoramica." Questioni di Economia e Finanza 198.
- Reed, C. (2007). "Taking Sides on Technology Neutrality." Script-ed 4(3).
- Russell, S. J., Norvig, P., & Davis, E. (2010). Artificial intelligence: a modern approach. 3rd ed. Upper Saddle River, NJ: Prentice Hall.
- SAE (2018). J3016_201806 - Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles. https://www.sae.org/standards/content/j3016_201806/, Society of Automotive Engineers.
- Salvini, P. (2013). Taxonomy of Robotic Technologies. Robolaw Grant Agreement Number: 289092, D4.1.
- Sesta, M. (2015). Filiazione (diritto civile). Enciclopedia del diritto. Milano. VIII., 445-479

- Smart Dubai (2019). AI Ethics principles & guidelines. Dubai: 16.
- Smit, J., S. Kreutzer, C. Moeller and M. Carlberg (2016). Industry 4.0, Brussels, European Parliament.
- Sollini, M., L. Antunovic, A. Chiti and M. Kirienko (2019). "Towards clinical application of image mining: a systematic review on artificial intelligence and radiomics. ." European Journal of Nuclear Medicine and Molecular Imaging 46(13): 2656–2672.
- Steer Davies Gleave (2014). Study on the Third-Party Liability and Insurance Requirements of Remotely Piloted Aircraft Systems. Brussel, European Commission.
- Stone, P., R. Brooks, E. Brynjolfsson, R. Calo, O. Etzioni, G. Hager, J. Hirschberg, S. Kalyanakrishnan, E. Kamar, S. Kraus, K. Leyton-Brown, D. Parkes, W. Press, A. A. Saxenian, J. Shah, M. Tambe and A. Teller (2016). One Hundred Year Study on Artificial Intelligence (AI100). https://ai100.stanford.edu/sites/g/files/sbiybj9861/f/ai100report10032016fnl_singles.pdf.
- Taleb, N. N. (2007). The Black Swan. Random House
- Till, A. L., S. Zahidi and V. Ratcheva (2016). The Future of Jobs Employment, Skills and Workforce Strategy for the Fourth Industrial Revolution, World Economic Forum. Available at http://www3.weforum.org/docs/WEF_Future_of_Jobs.pdf.
- Timan, T., R. Snijders, M. Kirova, S. Suardi, M. v. Lieshout, M. Chen, P. Costenco, E. Palmerini, A. Bertolini, A. Tejada, S. v. Montfort, M. Bolchi, S. Alberti, R. Brouwer, K. Karanilokova, F. Episcopo and S. Jansen (2019). Study on safety of non-embedded software. Service, data access, and legal issues of advanced robots, autonomous, connected, and AI-based vehicles and systems: final study report regarding CAD/CCAM and industrial robots. Brussel, European Commission.
- Tomasello, F. and M. Ducci (2016). Research for TRAN Committee: Safe Integration of Drones into Airspace. Brussels, European Parliament.
- United Nations (1999). UNCITRAL Model Law on Electronic Commerce Guide to Enactment with 1996 with additional article 5 as adopted in 1998. New York, United Nations Publication. Sales No: E.99.V.4.
- Vardi, M. Y. (2012) "Artificial Intelligence: Past and Future." Communications of the ACM 55.
- Vihinen, M. and C. Samarghitean, “Medical Expert Systems”, Current Bioinformatics (2008) (2008). "Medical Expert Systems." Current Bioinformatics 56(3).
- von Bar, C., E. Clive and H Schulte-Nölke et al (eds). & Research Group on the Existing EC Private Law. (2009). Principles (2009). Principles, Definitions and Model Rules of European Private Law Draft common frame of reference (Dcfr) (Full ed.). Munich, Sellier European Law.
- Wang, P. (1995). On the working definition of intelligence. Technical Report 94. Center for Research on Concepts and Cognition, Indiana University.
- Whittaker, M., K. Crawford, R. Dobbe, G. Fried, E. Kaziunas, V. Mathur, S. Myers West, R. Richardson and J. Schultz (2018). AI Now Report 2018, AI Now Institute, New York University: 8.
- WIPO (2019). WIPO Technology Trends 2019: Artificial Intelligence. Geneva, World Intellectual Property Organizat

This study – commissioned by the Policy Department C at the request of the Committee on Legal Affairs – analyses the notion of AI-technologies and the applicable legal framework for civil liability. It demonstrates how technology regulation should be technology-specific, and presents a Risk Management Approach, where the party who is best capable of controlling and managing a technology-related risk is held strictly liable, as a single entry point for litigation. It then applies such approach to four case-studies, to elaborate recommendations.

PE 621.926

Print ISBN 978-92-846-6108-4 | doi: 10.2861/981369 | QA-02-20-006-EN-C
PDF ISBN 978-92-846-6107-7 | doi: 10.2861/220466 | QA-02-20-006-EN-N