

Chapter Twelve

Who is accountable for the algorithm? Assessing the effectiveness of the EU's approach towards AI liability

PABLO MARTÍNEZ-RAMIL, TANEL KERIKMÄE

1. Introduction

The many challenges that AI systems possess for legal systems generated a wide debate in academia. The fast pace of R&D, along with the potential incorporation of these technologies into any human activity, made the list of potential challenges grow exponentially. The European Commission, seeing itself at the mercy of technological design choices taken beyond its borders, proposed in 2021 the AI Act. For the first time, part of the challenges posed by AI systems would be tackled through hard law, revolutionizing the digital regulatory landscape, and generating echoes in the legal systems of its digital counterparts.

In September 2022, a set of rules to address the civil liability of AI systems was proposed. Defined as “the two sides of the same coin,” the AI Act and the AI Liability directive intended to contribute to the establishment of a digital ecosystem of trust. A compendium of safety-oriented rules aimed at reducing risks and preventing damages accompanied by a liability regime that ensures an “effective and realistic” compensation.

The academia had previously approached from multiple angles the issue of AI responsibility, covering questions that range from the granting legal personality to AI systems to the definition of elements that hinder the establishment of criminal liability for AI malfunctioning.

This research, while finding its grounds in the preceding academic discussion, incorporates technical aspects attached to the AI life cycle to break down the notion of liability; defining and delimiting the role of the multiple actors involved to introduce a comprehensive understanding of the issue at stake. Against this backdrop, this chapter will assess the effectiveness of the legal reforms undertaken by the EU to accommodate the civil liability regime to the technical reality of AI systems.

It should come as no surprise that contemporary societies have seen in recent times the rapid expansion of AI systems, progressively transforming more and

more areas of our everyday lives and revolutionizing industries across the globe. And yet, along with its tremendous potential, these systems present complex legal and ethical challenges when facing regulatory landscapes rooted in analogue times. One core question, debated for years in the legal academic circles, reflects on the notion of liability when applied to AI systems. Who should be held accountable when an autonomous system causes harm or makes erroneous decisions?

Recognizing the urgency of the matter, the European Union (hereinafter EU) has taken proactive steps, negotiating, and drafting several legal initiatives that will shape the first comprehensive regulatory framework that will apply to AI systems deployed within its borders.

On June 14, 2023, with an overwhelming majority of 499 votes in favor, 28 against and 93 abstentions, the European Parliament adopted its final negotiating position on the Artificial Intelligence (hereinafter AI) Act (hereinafter AIA),⁶²³ *de facto* launching the “trilogue,” the interinstitutional negotiations between the Commission, the Council, and the Parliament. Barely two weeks later, some of the largest companies across the EU raised their concerns in an open letter to the EU lawmakers.⁶²⁴ The signing companies (such as Germany’s Siemens or France’s Airbus) claimed that, among other issues, the current approach taken by the AIA would “*jeopardize Europe’s competitiveness and technological sovereignty without effectively tackling the challenges we are and will be facing*” and involved “*disproportionate compliance costs and disproportionate liability risks*”.⁶²⁵

With their words, the signing companies were not only lobbying against the current state of the AI Act but also against two newly proposed legal instruments: the AI liability Directive (hereinafter AILD) and the Product Liability Directive (hereinafter PLD), for they all constitute a whole. This type of criticism has been constant since the early beginnings of the legislative process. And very often, the never-ending debate focused on the role of innovation and whether it promotes or hinders R&D. This will remain outside the scope of this chapter.⁶²⁶ Instead, the following sections will shed light on the specific

⁶²³ EUROPEAN PARLIAMENT. *MEPs ready to negotiate first-ever rules for safe and transparent AI*. European Parliament News, Press release, June 14, 2023 [online]. Available at:

⁶²⁴ TOH, M. ‘*Serious concerns*’: *Top companies raise alarm over Europe’s proposed AI law*. CNN Business, June 30, 2023, [online]. Available at:

⁶²⁵ NO NAME. *Open letter to the representatives of the European Commission, the European Council and the European Parliament. Artificial Intelligence: Europe’s chance to rejoin the technological avant-garde*. [online] Available at:

⁶²⁶ See, in this regard: LIU, H. Y., MAAS, M. M., DANAHER, J., SCARCELLA, L., LEXER, M., VAN ROMPAEY, L. *Artificial Intelligence and Legal Disruption: A New Model for Analysis. Law, Innovation and Technology*. vol. 12, no. 2, 2020, pp. 205–258.

issue of AI liability, delimiting the approach taken by the EU, and evaluating the recent proposals.

To that end, and based on prior academic discussions, this research explores the intersection of the AI life cycle, the actors involved in it, the proposed regulatory regime, and the determination of liability. It aims to offer a comprehensive understanding of the current legislative landscape while addressing it critically. In other words, this chapter will evaluate the EU's legal reforms and the effectiveness of its overall approach towards AI liability, exploring its key components, assessing its strengths and limitations, and discussing potential implications for accountability in the era of algorithmic decision-making.

2. Methodology

Ultimately, this chapter seeks to answer – to the extent that is possible – the question that names it: “Who is accountable for the algorithm?” Given its broad formulation and the many cornerstones of the topic, it has been narrowed to answer it considering the proposed EU legislation and the technical reality attached to these systems.

A detailed examination of the upcoming regime would deserve a much more extensive analysis than what this chapter would be able to provide. Instead, it intends to serve as a roadmap that will help others to navigate and approach the upcoming regime while acknowledging potential pitfalls.

To that end, this chapter departs from the prior discussion concerning AI and liability, defining the core concepts to this discussion, and introducing some of the main legal challenges that needed urgent regulatory attention. Section 4 continues addressing the technical aspects related to the AI life cycle and the many actors that can be involved in the process, essential to provide context and understand the complexities of AI liability. Section 5 covers the EU, the scope of their competences and a brief mapping of the regulatory initiatives that aim to establish a liability regime. It also digs into the liability regime implemented by the EU and provides an overview of how it applies in practice, in relation to the technical reality previously addressed and commenting on potential pitfalls, or the areas that -to the date- remain unaddressed by harmonization instruments. Section 7 closes this chapter providing some conclusions.

3. A recap on the discussion concerning AI and liability.

a) Defining AI.

Even if, by now, most of the readers will be already acquainted with the concept of AI, a brief commentary is in place. The recently approved compromised position on the AIA by the EU parliament defines it as: “*a machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions, that influence physical or virtual environments.*”⁶²⁷

In the original proposal, the Commission had its focus on the technical reality that imbued certain types of software and made them qualify as AI systems, adopting a dynamic approach that would allow the Commission to qualify new technical developments as AI.⁶²⁸ This partially obeyed to the historically loose character of its definition, often referred in the doctrine as the “AI effect.” In a few words, it came to express that, ever since Alan Turing allegedly coined the term for the first time in 1950, the concept itself evolved along with the state of art of the technology. Hence, when innovative technologies become mundane, they lose the “privilege” of qualifying as AI.⁶²⁹ With their latest approach, the definition took a more abstract turn, leaving aside the technical aspects and bridging the gap between the Commission’s approach and the one of the Organization for Economic Cooperation and Development (OECD).

Given the purposes of this chapter, the differences between the different types of AI techniques will not be examined.⁶³⁰ The definition employed here will follow the one of the EU parliament, understanding AI as a machine-based system (hence admitting both software and hardware) operating with different levels of autonomy (therefore encompassing in essence, the most widespread AI

⁶²⁷ Amendment 165. Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206–C9-0146/2021–2021/0106(COD)).

⁶²⁸ Art 3(1). Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts.

⁶²⁹ LIU, H. Y., MAAS, M. M., DANAHER, J., SCARCELLA, L., LEXER, M., VAN ROMPAEY, L. Artificial Intelligence and Legal Disruption: A New Model for Analysis. *Law, Innovation and Technology*. vol. 12, no. 2, 2020, pp. 215.

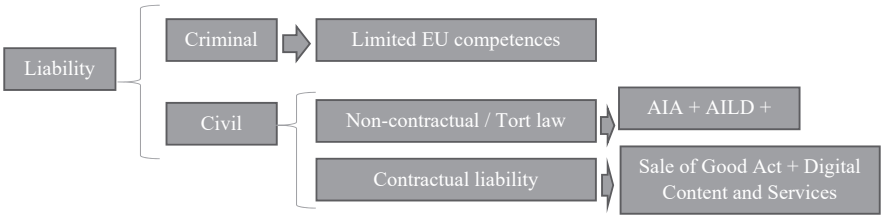
⁶³⁰ However, they are paramount to develop a more comprehensive understanding of the issue at stake. See, in this regard, MARTÍNEZ-RAMIL, P. Discriminatory algorithms. A proportionate means of achieving a legitimate aim? *Journal of Ethics and Legal Technologies*. vol. 4, no. 1, 2022, pp. 3–24.

techniques⁶³¹ – supervised, unsupervised, deep and reinforcement learning-) that produce outputs (with effects in the digital or the analogue world, or both) based on a given set of objectives (often called inputs).

b) Navigating the notion of legal liability.

The People’s Law Dictionary provides a concise yet clarifying definition of liability. In essence, it means “*legal responsibility for one’s acts or omissions*”.⁶³² The figure below simplifies the distinction between the types of liability and the relevant legal initiatives that apply to AI in the EU:

Figure 1: Types of liability and relevant EU legal initiatives



Civil and criminal liability typically reflect the responsibility arising from violations of private law (that governs relationship between people) and criminal law⁶³³ (ultimate expression of the monopoly on the use of force by the states, and to protect the public interests of a society).⁶³⁴

Several reasons explain the slow EU harmonization in criminal matters. The Treaty on the Functioning of the European Union (hereinafter TFEU) Art 67 establishes the obligation of ensuring a high level of security in the Union through “*coordination and cooperation*” between the relevant authorities, through “*mutual recognition of judgements in criminal matters*” and “*if, necessary, through the approximation of criminal laws*”. In a similar way, Art 82 (2) empowers the Parliament and the Council to establish minimum rules on criminal matters “*to*

⁶³¹ SARKER, I. H. Machine Learning: Algorithms, Real-World Applications and Research Directions. *SN Computer Science*. vol. 2, no. 160, 2021, pp. 1–2.

⁶³² HILL, G. N., HILL, K. T. *The People’s Law Dictionary. Taking the mystery out of the legal language*. New York: MJF Books, 2002, pp. 248–249.

⁶³³ TURNER, J. Robot Rules. Regulating Artificial Intelligence. Cham: Springer Link, Palgrave Macmillan, 2019, p. 82.

⁶³⁴ For the purposes of this research, this section will only refer to criminal and civil liability. Liability arising from administrative law related causes will be left aside, for the regimes are very specific to national realities.

the extent necessary to facilitate mutual recognition of judgments and judicial decisions and police and judicial cooperation".⁶³⁵ The primary law specifically refers to this type of harmonization through the prism of "necessity" to achieve the goals set in the treaties. This has led to a cautious harmonization in this area, understanding that criminal law is an expression of the sovereignty of the Member States that needs to be respected attending to the necessity principle. In other words, *"the more intrusive harmonization measures intervene in national criminal law systems, the more important they must be for achieving the Union's objectives"*.⁶³⁶

Hence, and while acknowledging the influence of EU law not only in the national legal systems but over their own interpretation, criminal law remains mostly under the control of Member States, that only need to observe obligations emanating from international law instruments that define the minimum standards (such as the European Convention on Human Rights)⁶³⁷ as well as their own constitutional rules. To the date, criminal systems among the Member States still differ. A good example -and of special relevance for AI systems- is the notion of hate crimes. Specifically, those not involving racism or xenophobia. While several countries regulated hate crimes against women and LGBT+ people, others do not offer the same level of protection across the EU.⁶³⁸ In absence of a specific harmonization measures in digital areas, an AI system (and specially, a general-purpose one -such as the (in)famous ChatGPT 4 or Bard-) might end up reflecting a conduct that, if it was a natural person the one committing it, would entail criminal liability. Moreover, in the context of hate crimes, the same conduct could raise legal questions in some Member States yet not in others.

As highlighted above, civil liability arises from violations of private law. Those might be (i) originated in a contractual relationship or (ii) not, also referred to as tort law. Within the meaning of tort law, several types are acknowledged across different legal regimes.

- Negligence: In a few words, the term refers to conducts that fail to perform to a required standard⁶³⁹. A conduct qualifying as a negligence presumes the

⁶³⁵ Arts 67 & 82(2), Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union. 2012/C 326/0.

⁶³⁶ SCHROEDER, W. Limits to European Harmonization of Criminal Law. *Eurocrim*. vol. 2, 2020, p. 147.

⁶³⁷ Art 52(3) identifies the Convention as the bare minimum that the Union can enhance through more extensive protection. Charter of Fundamental Rights of the European Union.

⁶³⁸ STUDY REQUESTED BY THE LIBE COMMITTEE. *Hate speech and hate crime in the EU and the evaluation of online content regulation approaches*. PE 655.135, July 2020, European Parliament, [online]. Available at:

⁶³⁹ NOLAN, D., DAVIES, J. Torts and Equitable Wrongs. In BURROWS, A. (ed.). *English Private Law*. Oxford: Oxford University Press, 2017, pp. 934.

existence of a duty not to cause, or to prevent a specific harm. That duty must have been breached and that breach must constitute the cause of the produced harm. Some legal systems include an extra circumstance to consider, the foreseeability of the damage⁶⁴⁰. The latter is of special relevance when dealing with AI systems that are progressively learning from their interactions with the users; for new types of interactions, inputs, or data hold the potential to alter the algorithmic decision-making process and therefore bring unforeseeable consequences.

- **Strict and product liability:** Typically, product liability is considered a type of strict liability. The former refers to a set of rules that define liability regimes when a specific product causes harm. The origin of the harm must come from a defect in the product itself. Strict liability refers to situations where liability arises (hence entailing legal consequences) in the absence of fault or criminal intention.⁶⁴¹ Traditional examples involve liability arising from the harm caused by the possession of very dangerous products (even when they are carefully stored), such as explosives, or wild animals.
- **Vicarious Liability:** Cases of vicarious liability refer imply the existence of responsibility for one person (the so-called “principal”) for actions undertaken by another (the “agent”). Typical examples involve a contractual relationship between employee and employer, or a hierarchical organization. The victim of the damage has the option to sue the principal for the actions of its agent, and later the principal will have (attending to the specific circumstances of the case) the option to act against its own agent for compensation.⁶⁴²

Contractual liability arises when there are specific provisions in a contract that outline the consequences in the event of a breach of obligations between two private parties, whether they are natural or legal persons.⁶⁴³ As shown in *Figure 1*, proposed and approved EU regulatory initiatives started to shape scenarios where civil liability arises from AI systems in both tort law and contractual law. They will be analyzed below.

⁶⁴⁰ TURNER, J. *Robot Rules. Regulating Artificial Intelligence*. Cham: Springer Link, Palgrave Macmillan, 2019, p. 86.

⁶⁴¹ *Ibid.*, p. 91.

⁶⁴² *Ibid.*, p. 100.

⁶⁴³ *Ibid.*, p. 109.

c) Questions that arise when analyzing Legal Liability originated in AI systems

In the previous section, the traditional types of liability have been delineated. Before addressing their “translation” into the EU regulatory landscape, this section will introduce some of the main elements that justified the legal discussion and the regulatory intervention.

In a nutshell, the legal liability of AI presents many challenges for contemporary legal frameworks, often rooted in analogue times. A significant one lies in determining who should be held responsible when an AI system causes harm or makes errors. Criminal liability traditionally revolves around natural persons, while civil liability affects both natural and legal persons. AI systems fall outside the scope of both definitions while holding a certain degree of autonomy. In 2017 the issue was debated in the European institutions, being finally disregarded.⁶⁴⁴ This autonomy is amplified in complex algorithms and decision-making processes (for instance, a Deep Learning Algorithm that is receiving real-time training from its own interactions with the users), making it challenging to trace and understand the exact cause of an AI-related incident.⁶⁴⁵ Although the issue of transparency and the black box⁶⁴⁶ will eventually disappear,⁶⁴⁷ the matter of accountability becomes more complicated when considering the diverse range of AI technologies and applications across various industries. In this regard, the number of liability questions that arise in healthcare contexts, or self-driving vehicles differ from the ones originated in a system designed to profile with advertisement targeting purposes.⁶⁴⁸

Different questions arise depending on the type of liability involved. For instance, under the prism of liability for defective products, it would not be clear “*whether the adaptive and dynamic nature of the AI through either machine-learning techniques, or updates, or revisions, may entail or create a defect*”

⁶⁴⁴ BURRI, T. *The EU is right to refuse legal personality for Artificial Intelligence*. Euractiv, May 31, 2018 [online]. Available at: <https://www.euractiv.com/section/digital/opinion/the-eu-is-right-to-refuse-legal-personality-for-artificial-intelligence/>. Accessed 12. 6. 2023.

⁶⁴⁵ MARTÍNEZ-RAMIL, P. Discriminatory algorithms. A proportionate means of achieving a legitimate aim? *Journal of Ethics and Legal Technologies*. vol. 4, no. 1, 2022, p. 7.

⁶⁴⁶ This term refers to the complicated decision-making processes in AI systems that are difficult for humans to understand and explain.

⁶⁴⁷ There are already strategies in place that allow to “open” the black box. See, in this regard, HACKER, P., CORDES, J., ROCHON, J. Regulating Gatekeeper AI and Data: Transparency, Access, and Fairness under the DMA, the GDPR, and Beyond. *Working Paper*. December 9, 2022, pp. 1–41.

⁶⁴⁸ See, in this regard, WACHTER, S. Affinity profiling and discrimination by association in online behavioral advertising. *Berkeley Technology Law Journal*. vol. 35, 2020, pp. 367–430.

in the AI system.⁶⁴⁹ If, instead, criminal liability of an AI system was the issue at stake, in addition to the problems highlighted above, the role of intentionality (*mens rea*), often core to the procedure in the definition of criminal conducts, would create questions that some consider not to be “even [...] solvable by our current legal system”.⁶⁵⁰ Nonetheless, it should be worthy of mention that similar debates have been going on for a while in relation to the controversial notion of Criminal Corporate Liability.⁶⁵¹

Lastly, it should be noted that alternative liability systems exist in the world and some authors even consider them legitimate alternative solutions for AI systems, such as the New Zealand’s Accident Compensation Corporation, a no-fault compensation scheme that reimburses the damages to victims of an accident regardless of “whether anyone was at fault”. It is financed through specific levies or taxes.⁶⁵² However, if such a regime were to regulate damage caused by AI systems in the EU, it could somewhat transform the internal market into a big sandbox, where the taxpayers would have to deal with the economic consequences of a harm produced by a malfunction of an AI system. Moreover, considering that AI developing companies already benefit from an unregulated landscape, where most of the data used to train the models is freely obtained through techniques such as data scraping,⁶⁵³ relying on their *bona fides* would not be prudent or sufficient to ensure ethical and responsible AI developing practices.

4. The AI life cycle and the actors involved in it.

Once disregarded the possibility of granting a new type of legal personality to AI systems, it becomes necessary to identify the actors involved in their development, for they will be the ones that could be held liable for potential malfunctions. The figure below simplifies the AI life cycle:

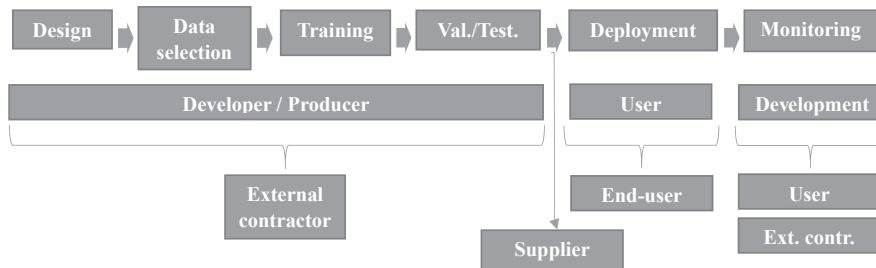
⁶⁴⁹ KARIKMÄE, T., MÜÜRSEPP, P., PIHL, H. M., HAMULAK, O., KOCHARYAN, H. Legal Person or Agenthood of Artificial Intelligence Technologies. *Acta Baltica Historiae et Philosophiae Scientiarum*. vol. 8, 2020, p. 86.

⁶⁵⁰ Ibid., p. 84.

⁶⁵¹ MARCIANO, A., BATTISTA RAMELLO, G. *Encyclopedia of Law and Economics*. Montpelier: Springer, 2019, pp. 391–392.

⁶⁵² TURNER, J. *Robot Rules. Regulating Artificial Intelligence*. Cham: Springer Link, Palgrave Macmillan, 2019, p. 102.

⁶⁵³ WES, D. & LAWLER, R. *Elon Musk blames data scraping by AI startups for his new paywalls on reading tweets*. The Verge, July 1, 2023 [online]. Available at: <https://www.theverge.com/2023/7/1/23781198/twitter-daily-reading-limit-elon-musk-verified-paywall>. Accessed 1. 7. 2023.

Figure 2. The AI life cycle and the potential involved actors, simplified⁶⁵⁴

Design: In a preparatory stage, the AI system is conceptually designed. Typically, the task lies in a developing company or producer that, either at their own expenses or attending a specific commission, determines the strategic steps to develop the system, which type of data will be necessary to train it, which model or algorithmic tool must be coded in light of the data, where will it be deployed...

1. **Data selection:** This stage involves both (i) the collection of datasets relevant to the purposes and tasks that the AI system will perform and (ii) the data cleaning and labelling (when necessary). While data cleaning aims at ensuring a certain level of data quality and integrity, labelling refers to different methods of data classification and is necessary for the development of supervised learning AI systems. This stage is key to ensure the correct functioning of the system; for biased, unrepresentative or uncomplete data sets will be reflected in the functioning of the system.⁶⁵⁵ It is not uncommon that these tasks are often subcontracted, being a third party the one in charge of the Data Selection phase.
2. **Training and Validation:** The datasets are usually divided into two groups: the training data set and the validating data set. Once the AI model has been developed and the data has been prepared, the system is trained with it. This process involves “feeding” the training data through the model, adjusting internal parameters, optimizing it to minimize errors... The model’s performance is then evaluated using the validating data set, defined metrics, and validation techniques. This way, its effectiveness and capacity to establish generalizations are assessed. Typically, it is the developing company the one in charge of the training and validating stages.

Once the system has been tested and considered to be ready for deployment, either the developing company itself or a third party acting as a supplier (for

⁶⁵⁴ For the purposes of this chapter, we will focus solely on the development of a Machine Learning system, excluding reinforcement learning due to its distinct applications.

⁶⁵⁵ HACKER, P. Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies Against Algorithmic Discrimination Under EU Law. *Common Market Law Review*. 2018, vol. 55, pp. 1146–1147.

instance, in cases where the AI is developed outside EU borders and enters the internal market) deals with the commercialization of the system.

1. **Deployment:** The deployment stage involves integrating the AI system into the intended environment or application. Depending on who will be in control of the AI, the literature often distinguishes between users and end users, being the latest the final user for whom the system was intended. For example, a company might acquire a license for an AI system that would allow them to implement an AI-powered chat-box for customer support. While they might be in control of the system (as “users”), the customers using the chat-box would constitute the “end-users”.
2. **Monitoring:** After an AI system is deployed, typically engineers work on optimizing the model’s performance, ensuring its compatibility with the deployment environment, and addressing any potential problems or challenges that could arise. Depending on the type of system, its complexity and its functioning, this task might be carried out by an external contractor, the developing company or the user piloting the deployment of the AI system.⁶⁵⁶

5. The EU approach towards regulating AI liability

5.1 Limits to the EU capacity

As is well-known, the EU draws its powers from primary law. Therefore, its capacity to regulate and harmonize is limited by the treaties.

Above, the reasons behind the limited harmonization in criminal matters were exposed. In addition, the TFEU Art 82 (2) also highlighted that any necessary harmonization on criminal matters through minimum rules must “*take into account the differences between the legal traditions and systems of the Member States*”.⁶⁵⁷ Extending criminal liability to AI systems or granting them a new type of legal personality would greatly exceed the capacities granted by primary law and could render its qualification *ultra vires*.

Conversely, the capacity to regulate civil liability for AI system lies in the TFEU Art 114, the legal basis for both the AIA and the AILD. The provision grants the EU the capacity to “*adopt the measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal*

⁶⁵⁶ MARTÍNEZ-RAMIL, P. Is the EU human rights legal framework able to cope with discriminatory AI? *IDP. Internet, Law and Politics E-Journal*. vol. 34, 2022, pp 3–5.

⁶⁵⁷ Art 82(2), Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union. 2012/C 326/0.

market”.⁶⁵⁸ This provision has been broadly interpreted, facilitating the adaptation of the internal market to the digitalization process that has been going on for years. Thus, it has been the legal basis for most of the digital regulatory initiatives promoted by the Von der Leyen Commission, such as the Digital Markets Act, or the Digital Services Act. The same provision justifies the existence of certain provision harmonizing contractual liability and product liability rules at the EU level, core to the notion of discussion on liability, as established above.

5.2 Relevant legislation.

Contractual liability.

Simply put, a contract constitutes a promise enforceable by law.⁶⁵⁹ It is the maximum expression of the legal principle of *pacta sunt servanda* and the principle of freedom of contract, only limited by concrete reasons of public interest. Therefore, any liability regime will be defined on a case-by-case basis, depending on the content of a specific contract.

The TFEU Art 4 (f) recognizes consumer protection as a shared competence between the EU and the Member States. In this regard, two instruments that aim at leveling the playing field between customer and seller deserve our attention, for they include provisions that limit contractual relationships and therefore influence the liability regimes included in contracts.

When AI systems are licensed through the cloud, they are referred to as Artificial Intelligence as a Service (AIaaS). The contractual relationships do not differ much from those governing Software as a Service (SaaS). The Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, includes some liability of the trader provision, establishes the burden of proof for breaches of Art 5 of the Directive on the trader (the stronger part of the contract), among other provisions.⁶⁶⁰

Conversely, if an AI system is sold as a good, the Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects

⁶⁵⁸ Art 114, Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union. 2012/C 326/0.

⁶⁵⁹ MEHREN, A. T. von. *Contract*. Encyclopedia Britannica, May 28, 2023 [online] Available at: <https://www.britannica.com/money/topic/contract-law>. Accessed 15. 6. 2023.

⁶⁶⁰ See, in this regard, Arts 11 & 12, Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services (Text with EEA relevance.) PE/26/2019/REV/1 OJ L 136, 22. 5. 2019, pp. 1–27.

concerning contracts for the sale of goods would apply. If the previous directive established certain liability standards for the trader, this one does the same on the seller. As the stronger part, the seller is also granted with the burden of proof in certain cases.⁶⁶¹

These two directives establish the minimum standards that contractual relationships concerning the sale of goods and the provision of services should comply with.

Non-Contractual liability. An overview of the AIA

Being at the center of the academic discussions surrounding AI regulation, the AIA constitutes the world's first comprehensive AI Law. At the time of writing this chapter, the so-called "trilogue" (EU inter-institutional negotiations) just initiated discussions, therefore rendering any in-depth examination of the proposed obligations outdated. And yet, some notes can be drafted regarding the liability system that intends to be established.

The AIA distinguishes between four types of AI systems, attending to the risk they possess:

- AI systems constituting an unacceptable risk. Considered a threat to safety and fundamental rights, the systems falling under this category are clearly banned, such as social scoring systems by governments.
 - AI systems qualifying as high-risk. These systems present a high risk due to their area of deployment and the consequences of their outputs, therefore being governed by a set of obligations defined in the law.⁶⁶²
 - AI systems with limited risk. These systems only need to comply with specific transparency requirements.
 - AI systems presenting minimal or no risk at all. The AIA allows their free use.⁶⁶³

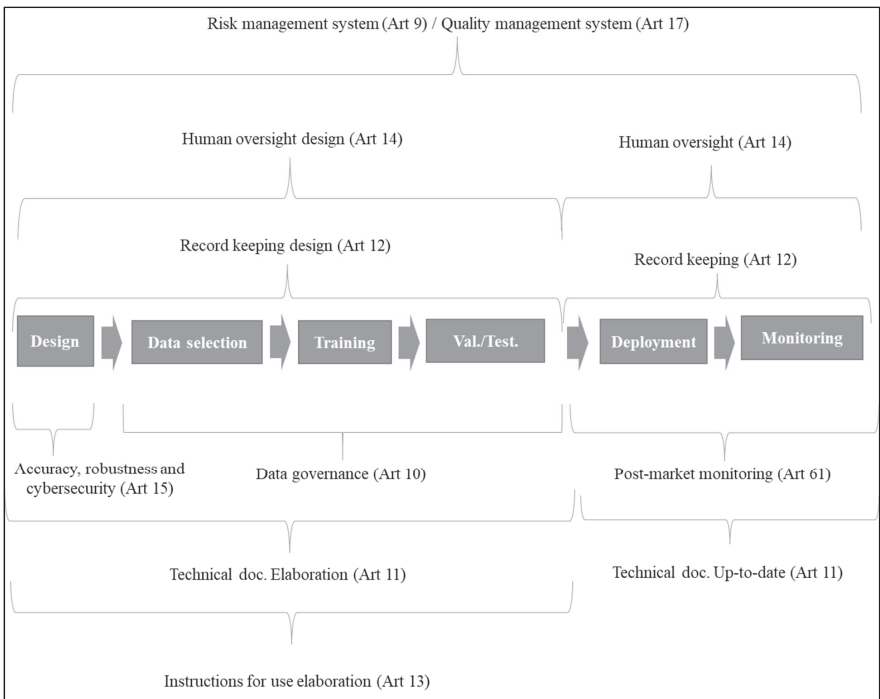
The figure below incorporates to the previously introduced AI life cycle the obligations imposed by the AIA to a high-risk AI system:

⁶⁶¹ See, in this regard, Art 10 & 11, Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC (Text with EEA relevance.) PE/27/2019/REV/1 OJ L 136, 22. 5. 2019, pp. 28–50.

⁶⁶² See, in this regard, *Figure 3*.

⁶⁶³ EUROPEAN COMMISSION. *Regulatory framework proposal on artificial intelligence*. Shaping Europe's digital future. European Commission, [online]. Available at: <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>. Accessed 14. 6. 2023.

Figure 3. An overview of the AIA obligations for high-risk AI systems through their life cycle.



In a few words, the AIA establishes several requirements that are connected to the risk that an AI system might possess. Ultimately, these requirements must be fulfilled by natural or legal entities, who can be held responsible in cases of non-compliance.

Art 71 of the proposed AIA established the system of penalties, that are imposed to “operators.” This term includes the “*provider, the user, the authorized representative, the importer and the distributor.*” They are defined in Art 3:

- Provider: means a natural or legal person, public authority, agency or other body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge.
- Small-scale provider: means a provider that is a micro or small enterprise within the meaning of Commission Recommendation 2003/361/EC 61.
- User. Any natural or legal person, public authority, agency or other body using an AI system under its authority, except where the AI system is used in the course of a personal non-professional activity.

- Authorized representative. Any natural or legal person established in the Union who has received a written mandate from a provider of an AI system to, respectively, perform and carry out on its behalf the obligations and procedures established by this Regulation.
- Importer. Any natural or legal person established in the Union that places on the market or puts into service an AI system that bears the name or trademark of a natural or legal person established outside the Union.
- Distributor. Any natural or legal person in the supply chain, other than the provider or the importer, that makes an AI system available on the Union market without affecting its properties.⁶⁶⁴

The original text of the proposal reserved in its Art 71 the highest penalties for operators that:

- Did not comply with the prohibition of AI qualifying as unacceptable risk.
- Did not comply with Art 10, Data Governance in the development of a high-risk AI system.

These fines, in their current wording, would involve a maximum of 30 million euro or up to 6% of the annual worldwide turnover if the operator is a company, whichever is bigger.

The noncompliance with the rest of the measures contained in *Figure 3*⁶⁶⁵ would entail fines of up to 20 million euro or 4% of the annual worldwide turnover if the operator is a company, whichever is bigger.

Lastly, noncompliance with Art 23 would involve fines of up to 10 million euro or 2% of annual worldwide turnover if the operator is a company, whichever is bigger.

Non-Contractual liability. The PLD and the AILD

As a stand-alone instrument, the AIA does not seem to open new paths for victims of an AI system to seek liability. The providers are the ones bound by the regulation, that need to ensure compliance in most cases through the – still controversial – self-conformity assessments.⁶⁶⁶ In other words, it only establishes some sort of EU administrative liability for these operators when it is revealed the lack of compliance with the relevant provisions.

⁶⁶⁴ Art 3. Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts.

⁶⁶⁵ In addition to Arts 19, 20, 21 & 22 of the proposed AIA.

⁶⁶⁶ See, in this regard, HACKER, P. *The European AI Liability Directives – Critique of a Half-Hearted Approach and Lessons for the Future*. arXiv preprint arXiv:2211.13960, November 25, 2022, pp. 1–72.

However, when addressed jointly with the AILD, the approach of the AIA somewhat reflects the type of tort liability known as “negligence”. In fact, the preamble to the proposed AILD refers to the term on two occasions. The AILD introduces a fault-based system that seeks to tackle the power unbalance between an end-user suffering harm from a specific AI-system and the operator of the system. It obliges the Member States to empower the courts to be able to obtain and disclose relevant evidence regarding a high-risk AI system suspected of having caused damage. Moreover, it establishes a presumption of a causal link in the case of fault if several conditions are fulfilled, opening the paths for potential victims to claim damages.

On the other hand, the proposed PLD addresses AI liability from a perspective of product liability. The key requirement for liability is the existence of a defect on the product. While the current PLD introduced many questions when facing digital assets, the newly proposed one incorporates them explicitly, listing elements that are strongly connected to the nature of AI systems. In this regard, when addressing the defectiveness of a product, references include:

- *the presentation of the product, including the instructions for installation, use and maintenance;*
- *the effect on the product of any ability to continue to learn after deployment;*
- *the moment in time when the product was placed on the market or put into service or, where the manufacturer retains control over the product after that moment, the moment in time when the product left the control of the manufacturer;*
- *product safety requirements, including safety-relevant cybersecurity requirements.*

If operated comprehensively and proportionately, these requirements can significantly improve the current standing of the product liability regime involving AI systems. But an explanation of how these elements will be measured is still missing, rendering any expectations futile at this point.

Another inclusion worth mentioning in the proposed PLD is the definition of “damage”, that now includes medically recognized harm to psychological health. This is of great significance, for it leaves the door open to address the legal challenge that recommendation algorithms in social media platforms constitute and the harm they cause to their users. Especially, because that might fall outside the high-risk qualification of the AIA.

Lastly, it should be noted that the proposed PLD Art 3 imposes a somewhat stricter transposition of the Directive in comparison to the AILD.⁶⁶⁷ And, although

⁶⁶⁷ Art 3 establishes that “Member States shall not maintain or introduce, in their national law, provisions diverging from those laid down in this Directive, including more, or less, stringent provisions to achieve a different level of consumer protection, unless otherwise provided for in

they share a similar wording in their respective Arts 8 and 3, the high reliance of the AILD on the AIA will necessarily entail certain modifications before assessing its full potential.

6. Conclusions. Who is accountable for the algorithm?

In conclusion, the implementation of the AI Act and the legal instruments analyzed represents a significant step towards regulating artificial intelligence and ensuring ethical and responsible AI practices. However, it must be acknowledged that, despite the obligations outlined in these frameworks, there are still potential instances where AI wrongdoings may occur, even in full compliance with the existing legal instruments. Acknowledging this reality can only leave a bittersweet taste, for there is no concrete answer that can give a closure to the proposed question.

Who is accountable for the algorithm? Well, it depends. There are no systems of criminal liability for AI in place, and, although it is only a matter of time before we see them occupy the headlines, it is not clear whether the current legal landscape can tackle the questions that will come. The arguments exposed above reinforce this view.

In exploring non-contractual civil liability, previous research has shown that AI systems can still cause harm to users, even when complying with the AI Act. Instances such as proxy discrimination highlight this concern. In an ideal scenario of implementing the AI Act and the AI liability regime, three conditions would need to be met to establish liability: the harm must be caused by a high-risk AI system, a breach of the AI Act's obligations must be proven, and a causal connection between the breach and the harm must be demonstrated. If no breach occurs, the Product Liability Directive (PLD) may be the applicable instrument. Under the PLD, the defectiveness of an AI system will be assessed considering the listed circumstances in Article 6. How these requirements are balanced by the relevant authorities will significantly impact the outcome.

Lastly, it should be highlighted that neither the AIA, the PLD, or the AILD will keep their current wording unaffected. The results of the inter-institutional negotiations on the AIA will necessarily have an impact on the AILD, while the PLD will have to undergo its own procedure. The intention of this chapter was none other than to provide an overview of the state of the art. Only future research will be able to examine and study the established regime built upon the final form of these initiatives.

this Directive". Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on liability for defective products. COM/2022/495 final.