Original scientific paper

# LIABILITY IN A DIGITALIZED WORKPLACE: THE ROLE OF THE EU'S NEW AI FRAMEWORK BETWEEN INNOVATION AND SECURITY[*]

**Šime Jozipović, PhD, Assistant Professor**
University of Split, Faculty of Economy
Cvite Fiskovića 5, 21000 Split, Croatia
sjozipov@efst.hr

**Trpimir Perkušić, PhD, Assistant Professor**
University of Split, Faculty of Law
Domovinskog rata 8, Split, Croatia
trpimir.perkusic@pravst.hr

***ABSTRACT***

*The AI Act, adopted by EU lawmakers in 2024, marks a major step in harmonizing AI regulation across Europe by introducing a risk-based framework for AI system oversight. However, it does not directly address civil liability related to the implementation of AI based systems and technologies. To bridge this gap, the EU has taken steps by updating the Product Liability Directive (PLD) and negotiating the proposed Artificial Intelligence Liability Directive (AILD). The PLD now covers damages caused by products that use AI-systems, while the AILD is still under discussion. Despite these efforts, liability rules remain fragmented, particularly in workplace settings.*

*This paper explores how emerging EU legislation affects liability for AI-related damages at work, where clear rules are essential to ensure accountability and build trust in automation. It addresses challenges such as AI opacity, causation, and the balance between innovation and legal responsibility. Using examples like medical diagnostics and autonomous machines, the paper highlights the difficulties of assigning liability among employers, employees, and AI developers. It focuses on the intersection of contractual distribution of responsibilities, requirements under the AI act and special obligations of employers towards their employees.*

*Croatia's legal framework on contractual liability serves as a case study, focusing on how EU regulations intersect with national law and worker protection rules. The analysis reveals gaps in liability allocation, shows how guidelines for AI use will increase in importance and suggests how national and EU laws must adapt to support safe and lawful AI use in the workplace.*

***Keywords:*** *AI Act, damages, liability, workplace*

[*] This paper is a product of work that has been fully supported by the Faculty of Law, University of Split, under the project nr. 3. "Challenges of modern labor law - de lege lata and de lege ferenda (IMRP).

# 1. INTRODUCTION

The introduction of the European Union's Artificial Intelligence Regulation (AI Act) in 2024[1] marked a pivotal moment in AI regulation. As part of the EU's broader AI framework, this legislation seeks to harmonize rules governing the development, deployment, and accountability of AI systems. The Act introduces a layered, risk-based approach, categorizing AI systems based on their potential risks to safety and fundamental rights, and establishing compliance obligations proportionate to those risks.[2]. However, it does not directly address civil liability, which still remains fragmented in the European Union.[3] To close this gap, the European legislator has modernized the Product Liability Directive (PLD)[4] and had proposed the Artificial Intelligence Liability Directive (AILD).[5] The PLD now covers damages caused by products that use AI systems, while the AILD was withdrawn in early 2025 due to a lack of consensus among stakeholders. As a result, efforts to create a harmonized fault-based liability regime for AI have stalled, leaving gaps, especially in workplace settings.

Establishing clear liability frameworks among stakeholders is critical to fostering trust in AI technology, especially in workplaces integrating automation and robotics[6]. Employers as AI deployers must understand their roles and obligations for AI-based systems to be seamlessly integrated. This paper examines how evolving regulations shape liability distribution in the workplace.

It begins by analysing the EU's legislative efforts to balance innovation with accountability and security. Key challenges are identified, including the opacity of AI decision-making, difficulties in establishing causation, and competing interests

[1] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013 (in the following text AI Act).

[2] Ebers, M *et al.*, *The European Commission's Proposal for an Artificial Intelligence Act— A Critical Assessment by Members of the Robotics And Ai Law Society* (RAILS), J 4, No. 4, 2021, p. 593 f, 603.

[3] Montagnani, M. L.; Najjar, M. C.; Davola, A., *The EU Regulatory approach(es) to AI liability, and its Application to the financial services market*, Computer Law & Security Review, Volume 53, 2024, p. 6; European Commission: Directorate-General for Justice and Consumers, Liability for artificial intelligence and other emerging digital technologies, Publications Office, 2019, available at: [https://data.europa.eu/doi/10.2838/573689], Accessed 1 April 2025, p. 15.

[4] Proposal for a Directive of the European Parliament and of the Council on liability for defective products, COM/2022/495 final, adopted through Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products [2024] OJ L, 2024/2853.

[5] European Commission, "Proposal for a Directive of the European Parliament and of the Council on Adapting Non-Contractual Civil Liability Rules to Artificial Intelligence", Brussels, 28.9.2022 COM/2022/496 final.

[6] Ebers *et al.*, *op. cit.*, note 3, p. 594 f.

among AI developers, employers, their clients and employees. The tension between protecting intellectual property and the need for transparency in liability claims is also explored. Workplace-specific legal challenges, such as those involving machine learning based predictive models, autonomous vehicles and industrial robots, are examined to illustrate the complexities of assigning responsibility among employees, employers, and third-party providers.

The paper then uses Croatia's workplace liability framework to demonstrate how the new EU legislation impacts AI-related damages in the workplace. The analysis highlights Croatia's employer-employee liability rules, obligations under worker protection laws, and general civil law principles in AI-driven scenarios. It focuses on contractual damages and scenarios involving employers as the central node between their AI providers, clients and employees. By situating Croatia's legal framework within the broader EU context, the paper identifies regulatory gaps and offers insights into how liability laws may evolve to support both technological innovation and legal certainty in an increasingly digital workplace.

## 2. THE EUROPEAN UNION'S LEGAL FRAMEWORK FOR ARTIFICIAL INTELLIGENCE

Regulating new technologies is inherently difficult. Legal norms concerning new technology are frequently created at a time when the technology is still evolving, often before its full implications are known or specific issues can be clearly anticipated. However, when a new technology has a strong economic or social impact, it is reasonable to approach regulation even in this early phase, in order to create legal certainty and mitigate risks.[7] This is also in line with consultations which have shown a strong support for the establishment of clear regulations that ensure liability in cases where intangible products used to operate hardware are defective and cause physical/property damage.[8]

In this context, AI regulation is important, but in fact poses an even greater challenge than the regulation of other new technologies. AI technology is not only rapidly advancing, but AI systems are also capable of learning, adapting, and mak-

[7] Arcila, B. B., *AI liability in Europe: How does it complement risk regulation and deal with the problem of human oversight?*, Computer Law & Security Review, Volume 54, 2024, p. 2.

[8] European Commission Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs (DGGROW)Directorate-General for Justice and Consumers (DG JUST): Adapting Civil Liability Rules to the Digital Age and Artificial Intelligence - Factual summary report on public consultation, Ref. Ares (2022)2620305 - 06/04/2022, Available at: [https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Civil-liability-adapting-liability-rules-to-the-digital-age-and-artificial-intelligence/public-consultation], Accessed: 1 April 2025 p. 3.

ing decisions in ways that may be opaque even to their developers. This dynamic and autonomous nature of AI complicates traditional legal approaches based on clear accountability and predictability. An important issue the EU legislators faced when designing the new AI framework was balancing between security and innovation. In this context an especially challenging but crucial aspect of regulation concerns the question of responsibility for damages caused by an AI-operated device or service. In the case that the producer of an AI was free of accountability, there might be no incentive to provide good product or service and it could damage people's trust in the technology. However, overly strict liability could prevent innovative solutions to emerge.[9]

## 2.1. THE AI ACT

As a result of the increasing relevance of artificial intelligence in business and society, the European Commission has worked on the implementation of a comprehensive AI framework. The cornerstone of the new AI framework was the proposal of the Regulation Laying Down Harmonized Rules On Artificial Intelligence[10], which later entered into force in July of 2024 as the already mentioned AI Act. At its core the Act establishes a risk-based regulatory regime for AI systems, imposing stringent *ex ante* obligations on AI developers and users with the aim to ensure a safe, transparent and individual rights oriented use and application of AI.[11] It however does not establish a civil liability regime for AI-related damages[12]. If an AI system malfunctions or produces a harmful outcome – for instance, an autonomous robot injuring a factory employee, an AI medical tool giving a fatal recommendation, or an algorithm unlawfully denying someone employment – compensation regimes for damages are governed by existing liability laws like tort law, product liability law, or contract law.

The AI Act defines key actors in the AI space, namely:[13]

[9] Artificial intelligence: threats and opportunities, available at: [https://www.europarl.europa.eu/topics/en/article/20200918STO87404/artificial-intelligence-threats-and-opportunities], Accessed 1 April 2025.

[10] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM(2021) 206 final, Brussels, 21 April 2021. This proposal was subsequently adopted as Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, and (EU) No 168/2013 (Artificial Intelligence Act), OJ L 168, 30 June 2024., p. 1–152 – the so called AI act.

[11] Montagnani *et al., op. cit.,* note 4, p. 8; Ebers e*t al.*, *op. cit.*, note 3, p. 595.

[12] Ebers *et al., op. cit.*, note 3, p. 599.

[13] Art. 3 para. 1 nr. 3 – 7 AI Act.

- AI provider –any person or body – public or private that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge;
- AI deployer –any person or body – public or private that uses an AI system under its authority except where the AI system is used in the course of a personal non-professional activity;
- AI related authorised representative - any natural or legal person located or established in the Union who has received and accepted a written mandate from a provider of an AI system or a general-purpose AI model to, respectively, perform and carry out on its behalf the obligations and procedures established by this Regulation;
- AI importer –any natural or legal person located or established in the Union that places on the market an AI system that bears the name or trademark of a natural or legal person established in a third country;
- AI 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;

It is important to note, that multiple entities can have the status of AI provider. If for example a deployer makes substantial modification to the system or embeds the system in a larger product, he assumes provider responsibilities.[14] Thus it is important to assess if a deployer primarily uses AI systems, or substantially modifies them, in order to determine their status, and thus obligations under the AI act. This is especially important, as the AI act determines EU wide standards for the aforementioned actors, and thus can provide a benchmark of proper care, that can then be used under proposed European or domestic AI liability law. In the context of this paper, it is especially important to note that under the AI Act, employers can qualify as AI deployers when they use AI systems in the context of their professional activities but also as providers if they significantly alter existing systems. Employees, on the other hand cannot be considered deployers. They can have a dual role: they can be affected persons when subject to decisions or evaluations made by AI systems, and they can be the human operators who directly interact with or oversee AI systems as part of their work obligations.

[14] See explanation in rec. 84 f. AI Act.

## 2.2. AI SYSTEM RISK CATEGORIES

In order to understand the obligations of each group of actors, it is necessary to understand how AI related risks are defined under the Regulation. The AI act aims to establish extensive regulation on those types of AI systems that pose a concrete risk, and avoids putting an additional regulatory burden on low/no risk AI systems.[15] Under the AI Act, two types of AI systems are explicitly defined: Prohibited AI systems and High-risk AI systems.

Prohibited AI systems include all AI systems that are applied in a manner that is considered to be individual rights to an extent that is considered unacceptable in the EU. Examples include social scoring mechanisms, the use of AI to manipulate individuals and vulnerable groups etc.[16] In the context of AI-related damages and the employer-employee relationship, it is important to note that the use of such prohibited systems already constitutes a legal violation—and if this use results in harm, it may form the basis for a claim by the injured party. However, the focus of this paper is not on cases where AI systems are used unlawfully per se, but rather on situations where legally permitted AI systems malfunction, are misused, or produce harmful outcomes, raising questions of liability, responsibility, and redress within the employment context. Therefore, the category of high-risk AI systems in contrast to other legal AI systems is especially important.

Under the term high-risk AI systems fall all AI systems that are related to sensitive sectors, services or products that require an enhanced level of regulatory compliance. This applies both for situations where the AI is the product, or where it is a part of the product that is related to the product's safety aspects[17]. The category of high-risk AI system especially covers those AI systems that could have an impact on the health, safety or fundamental rights of natural persons, including by not materially influencing the outcome of decision making.[18] Examples include the use of AI in biometrics, critical infrastructure, essential services or law enforcement[19]. However, in the context of employment law it also includes hiring and workers' management. High-risk systems in this context are those systems that are intended to be used for the recruitment or selection of natural persons, in particular to place targeted job advertisements, to analyse and filter job applications, and to evaluate candidates. The same applies to AI systems intended to be used to make decisions affecting terms of work-related relationships, the promotion or termination of work-related

[15] Recital 46 AI Act.

[16] Art. 5 AI Act; Ebers *et al.*, *op. cit.*, note 3, p. 591 f.

[17] Art. 6 para. 1-2 in relation to Annex I, Annex III AI Act.

[18] Art. 6 para. 3 AI Act.

[19] Annex III AI Act.

contractual relationships, to allocate tasks based on individual behaviour or personal traits or characteristics or to monitor and evaluate the performance and behaviour of persons in such relationships.[20] However, if workers use AI systems as part of their work, this doesn't automatically qualify them as separate high-risk systems. Thus it is important to consider each system under the general rules of the AI act.

It is important to note that general purpose AI systems with extensive capacities have a specific position within the AI act. While these systems may not be directly aimed at any high risk activity, they could be used for high-risk activities due to their versatility. This could happen either directly, or through significant adjustments. Therefore the AI act requires that under any potentially significant change, a re-assessment of the risk level is conducted.[21] This solution, while putting an additional administrative burden on actors that make changes to an AI-system, was considered a necessary counterbalance to limiting strict regulation to high-risk systems, ensuring a layered approach.[22] Besides prohibited AI systems and high-risk AI systems, a specific third category exists. Namely AI systems that directly interact with natural persons and which are considered to be a limited-risk and need to fulfil various disclosure requirements.[23] These systems aren't considered to be seriously harmful as long as it is made clear that they are being used.[24]

## 2.3. OBLIGATIONS OF AI PROVIDERS UNDER THE NEW AI FRAMEWORK

The AI act aims at putting the main responsibility concerning AI systems on AI providers. These actors are working on developing the AI systems and thus are closest to its structure and programming. Therefore, they have the most direct insights into the workings of the system and are best suited to test, adapt and upgrade the system. As a result, it is their role under the AI Act to ensure AI systems are trustworthy before and during deployment.[25] The majority of responsibilities of AI providers are connected to high-risk AI systems, and they include: 1) Risk assessment and risk management, 2) Data Governance and Technical Documentation, 3) Transparency and Human Oversight Measures, 4) Post-Market Monitoring and Incident Reporting.

[20] Nr. 4 Annex III AI Act.

[21] Ebers *et al.*, *op. cit.,* note 3, p. 594.

[22] Philipp, H., T*he European AI liability directives – Critique of a half-hearted approach and lessons for the future*, Computer Law & Security Review, Volume 51, 2023, p. 10.

[23] Art. 50 AI Act.

[24] Another notworthy but less relevant category for this paper are so called general-purpose AI models which due to their capacities present a systemic risk. See: Art 51 f. AI Act.

[25] Ebers *et al.*, *op. cit.,* note 3, p. 597 f.

Providers have the duty to establish a rigorous risk management system throughout the AI's lifecycle. This means that they have the obligation to extensively test the system before it enters the market and from that point onwards to ensure continuous processes to identify, evaluate, and mitigate risks of harm or discrimination.[26] Safety measures must be adequate and proportionate, taking into account the specific risks of the system and the state of the art safety, accuracy, robustness, and cybersecurity requirements.[27]

Providers furthermore have to ensure a high level of training and input data that is sufficiently representative and as far as possible free of errors or bias to minimize risks to fundamental rights[28]. While it is practically impossible to provide perfect data to a model, in academia it is considered that the benchmark should be that data has to be collected and provided with a reasonable level of care.[29]

In the context of this paper, it is especially important to note that providers must also maintain extensive technical documentation and logs detailing the AI system's design, testing, and performance metrics.[30] This documentation can serve as evidence of due diligence and must be supplied to regulators or courts if needed. AI models are heavily reliant on the data imputed by the operator, as even high quality models cannot provide reliable results if they are based on faulty information.[31] Therefore, documentation will play a crucial role in the process of allocating responsibility.

A further important requirement is that AI providers have to ensure that the system is built with appropriate human oversight mechanisms which can effectively be used by deployers, for whom providers must make available clear instructions for use.[32] This is especially important in an employment context, as employees must receive clear instructions and sufficient training to operate AI systems. In academia, it has however been questioned if it is even possible to provide effective human oversight for very complex AI systems that are hard to fully comprehend.[33] Therefore, it remains to be seen to which extent the broad requirements of human oversight will work in practice, and in particular concerning the distribution of responsibility in liability cases. For example, if a provider fails to include a necessary human override and injury results, that omission may be deemed negligent

[26] Art. 8,9 AI Act.

[27] Art. 15 AI Act.

[28] Art. 10 AI Act.

[29] Ebers *et al.*, *op. cit.,* note 3, p. 595 f.

[30] Art. 10, 11 AI Act.

[31] Montagnani *et al.*, *op. cit.,* note 4, p. 3.

[32] Art. 14 AI Act.

[33] Ebers *et al.*, *op. cit.,* note 3, p. 596.

or render the AI "unsafe". An AI deployer could in contrast be liable if despite of clear instructions and a functioning human oversight mechanism, no actions have been taken to prevent damages. But it is to be expected that for most cases in practice the distribution of fault will not be this clear.

After deployment, providers must monitor the AI system's performance any incident that leads to death or serious harm to health, significant property damage, or serious disruption of critical services (serious incident). If such an incident occurs, the provider must inform regulators within 15 days and investigate the root cause.[34] This mirrors obligations in sectoral safety laws and creates a paper trail that could be vital in civil litigation. For example, if an autonomous AI medical device caused injury, the incident report would document the failure and provide useful evidence for an injured patient's claim. Notably, compliance with these duties does not automatically exempt a provider from liability; but non-compliance can trigger regulatory sanctions and bolster a victim's case that the provider fell below expected standards.

## 2.4. THE RESPONSIBILITY OF AI DEPLOYERS UNDER THE AI ACT

As mentioned above, the term "deployers" includes businesses using commercially available AI tools and systems, but not directly employees who are natural person operators[35] of the system under the mandate of their employers. Deployers of high-risk AI systems have clear obligations under the AI Act, which complement the provider's duties and aim to ensure safe and lawful use of AI in context. Key obligations on deployers include:[36] a) using the systems in accordance with instructions, b) assigning human oversight and monitoring, c) ensuring input data quality, d) record-keeping, e) transparency to affected persons and f) special obligations for employers who deploy AI systems.

While AI providers must provide deployers with clear instructions for use of AI systems, it is the responsibility of deployers to follow the provider's instructions and only use the system for its intended purpose and within the conditions the provider envisaged. They are required to take appropriate technical and organizational measures to ensure compliance with the usage guidelines.[37] This means that the use of an AI system has to be in line with its intended purpose. For example, if the provider specifies that an AI-powered diagnostic tool is only validated for adult patients, a deployer (hospital) should not use it for children without further

[34] Art. 73 AI Act.

[35] Art. 26 para. 2 AI Act.

[36] Art. 26 AI Act.

[37] Art. 26 para. 1, 3 f. AI Act.

validation. Failure to heed instructions could not only violate the regulation but also amount to negligence if harm results. However, it also determines certain aspects of the relationship between deployer and natural persons who use AI systems on their behalf like it is the case in employer-employee relations.

An especially relevant requirement for employer-employee relations is the obligation that every deployer of a high-risk AI must assign natural persons to exercise human oversight over the AI's operation[38]. These human overseers should have appropriate competence, training, and authority to interpret the system's outputs and intervene when necessary. The deployer is responsible for ensuring these individuals (e.g. operators, employees) understand the AI's limitations and can effectively supervise it. In addition, deployers are required to monitor the AI system's performance during actual use and suspend its use if it behaves anomalously or poses a significant risk.[39] It is the duty of the deployer (employer) to ensure that a competent natural person is assigned a task. Thus education and training responsibilities fall on the deployer. If the AI's use leads to a serious incident or malfunctions in a way that risks harm, the deployer must inform the provider or distributor without undue delay and even notify authorities if the provider cannot be reached.

An important aspect of AI systems is their use of new data. Thus in cases where the deployer inserts data into the AI system, the Act requires that input data be relevant, correct and representative of the intended use. A deployer cannot, for instance, use biased or incoherent data with a high-risk AI without potentially skewing its results. Doing so would violate the Act and likely be considered negligent if it causes harm. Even a well-built AI can produce harmful outcomes if supplied with flawed data. It is likely that especially in this aspect many questions concerning the factual responsibility for harmful outcomes will come from. Namely, AI system providers could defend their position by claiming faulty data being the reason for a harmful outcome, while deployers could either challenge this position or consider the fault of the natural person imputing the data (for example a negligent employee).

In order to identify faults and resolve potential dispute like those presented in the previous paragraph, deployers must keep logs generated by the AI system, to the extent those are under their control, for a period at least six months or longer if required by other law.[40] This obligation aims at ensuring a multi-level responsibility on creating sufficient evidence and complements the obligation of deployers of AI systems.

[38] Art. 26 para. 2 AI Act.

[39] Art. 26 para. 5 AI Act.

[40] Art. 26 para. 6 AI Act.

When deployers are employers using high-risk AI in the workplace, the AI Act requires that employers inform and consult their workers or their representatives before putting a high-risk AI system into use that will impact worker. This could cover AI systems for monitoring productivity, automated scheduling, or decisions to establish or end an employment contract. The deployer must notify individuals that an AI system is involved in decision-making and provide understandable information about the AI's intended purpose and how it affects them, especially in an employment context[41]. For example, if an employer uses an AI tool to screen job applicants or an AI system rates employees' performance, the applicants or employees should be informed of this automated processing and its logic in general terms. EU employment law already obliges employers to consult works councils or staff on significant technological changes[42] while the European Court of Human Rights has made clear that employee monitoring activities need to be disclosed to employees[43]. Therefore the AI act obligations create only an additional protection for employee rights without prejudice to existing measures.

## 2.5. CLASSIFYING AI USED IN THE WORKPLACE UNDER THE NEW AI BASED RISK CATEGORIES

As has been described above, the roles and obligations of the different actors in the AI space vary significantly based on the risk level of an AI system. Thus, it makes sense, first to give clear examples of AI systems commonly used in the workplace, and their classification. Here we can first differentiate between AI systems that are software products or part of software products and AI-systems integrated into hardware. AI software products can be used for various tasks like data analysis, optimization of processes, diagnostics, generating of various outputs like text, pictures, videos, reports etc. However, for the purposes of this paper it makes most sense to cover a number of key examples of AI systems, namely those used for: 1) low risk tasks like warehouse logistics, 2) assessment software related to work performance and employee tasks, 3) expert tasks like medical diagnostics or 4) generative tasks like the creation of graphic design elements. Simultaneously, we can consider cases of integrated AI systems in hardware like 5) self-driving vehicles, 6) autonomous industrial robots and 7) adaptable heavy industrial machines.

[41] Art 26 para. 7, recital 57,92 AI Act.

[42] See Directive 2002/14/EC of the European Parliament and of the Council of 11 March 2002 establishing a general framework for informing and consulting employees in the European Community, particularly Article 4(2)(e), which includes consultation on decisions likely to lead to substantial changes in work organisation or contractual relations, including the introduction of new technologies.

[43] See: *López Ribalda and Others v. Spain* [2019] ECHR 752, Applications Nos. 1874/13 and 8567/13, Grand Chamber Judgment of 17 October 2019.

Warehouse logistics optimization software is in general considered low risk. For example, if in a large distribution centre, an AI-driven system dynamically plans pick-and-pack routes for warehouse staff based on real-time inventory levels and order priorities, it doesn't affect fundamental rights. It also doesn't fall within one of the activities listed in Annex III of the AI Act; it merely optimizes internal processes without direct safety or rights implications. However, as it significantly affects the way employees will complete their work processes, it still would require the employer to discuss the implementation of such a system with the employee representatives and inform employees about the implementation. Furthermore, in case that it delegates tasks based on employee performance, the classification would be considerably different;

Especially in the context of this paper, an important type of AI system is related to employee performance evaluation software. This type of software can for example be used to score the time effectiveness of warehouse workers or sales agents' email response times and customer-satisfaction metrics to inform bonus allocations. As HR decision-making and employee evaluation software directly affects employees' rights and is directly mentioned under Annex III to the AI Act, it falls in the category of high risk software.[44]

In contrast to the previously mentioned tasks, assessment and prediction software can be a type of high risk software, for example when used to execute highly regulated expert tasks with a strong impact on individual rights, like it is the case in the medical sector. For instance, if a radiology department uses an AI model to analyse chest X-rays and flag potential pulmonary nodules for a clinician's review, the AI model would be considered high risk, as it is simultaneously strongly impacts individual rights and is used for medical device purposes which are explicitly covered by Annex I to the AI act.[45]

Generative graphic design software is generally not considered high risk. However, it can be linked to additional obligations on the deplorer's side, in order to prevent creating misleading content. For example, in cases where a marketing team uses an AI tool to generate layout suggestions, pictures of consumers using a product and visual assets for social-media campaigns, with designers refining the outputs. Such a system is not high risk *per se* but it must comply with transparency obligations (disclosure that content is AI-generated).[46]

[44] Art. 6 para. 1 and Annex III para. 4.

[45] Art. 6 para. 1 and Annex I nr. 13 AI Act.

[46] Art. 50 AI Act.

Many hardware products are more complex as they combine regular software, sensors, AI systems and simple hardware elements.[47] Therefore, their regulation will often be based on multiple legal sources. For example, (self-driving) vehicles are by themselves highly regulated.[48] Furthermore, a key component of AI used in these products is aimed at safety and security of passengers and third parties. Thus, AI systems used in these products fall clearly under the category of high-risk AI systems. Workers will for example use self-driving cars either as a passenger or in an oversight role / backup driver. They however also might use them to automatically transport equipment from one location to another, without themselves being a passenger. In all these cases, the AI operating these vehicles is considered a high-risk AI system.

Similar, when AI systems are designed to operate industrial robots or heavy machinery they will likely fall within the category of high-risk system due to these hardware products likely being covered under Annex I and the role of the AI system being directly linked to operations, and thus product safety.[49]

## 3. THE AMENDMENT TO THE PRODUCT LIABILITY DIRECTIVE

Civil law compensation for damages in the EU has largely not been harmonized with the exception of specific areas of law relevant to the single market[50] like product liability[51] or infringements to data protection law[52] and competition law.[53] While the PLD does not directly regulate workplace related damages, it is important to under-

[47] It is however also worth noting the Motor Insurance Directive (MID). This directive does not directly impact the distribution of liability, but provides rules concerning the liability insurance cover and thus have to be considered together with national tort law and thus would be an additional element of regulation. See: Directive 2014/104/EU of the European Parliament and of the Council of 26 November 2014 on certain rules governing actions for damages under national law for infringements of the competition law provisions of the Member States and of the European Union, OJ L 349, 5 December 2014, p. 1–19; European Commission, *op. cit.*, note 4, p. 16.

[48] Annex I nr. 14, 18 AI Act.

[49] Annex I Nr. 1 AI Act.

[50] European Commission, *op. cit.*, note 4, p. 16.

[51] Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products (recast) [2024] OJ L, 2024/2853.

[52] 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 May 2016., p. 1.

[53] Directive 2014/ 104/ EU of the European Parliament and of the Council of 26 November 2014 on certain rules governing actions for damages under national law for infringements of the competition law provisions of the Member States and of the European Union, OJ L 349, 5 December 2014, p. 1.

stand how the role of AI related damages for defect products are regulated, in order to understand the responsibilities and obligations of all parties involved.

The AI act mentions explicitly the Product Liability Directive in its recitals, as these two legal sources are meant to complement each other[54]. However, the PLD represents an independent improvement on existing product liability regulation which now includes AI related products[55]. If an AI system meets the broad definition of "product" the PLD is applicable and the revised PLD, includes software and by extension AI systems. Under the revised PLD, a person injured by a defective product can sue the producer without fault. It is thus essential for the injured party to establish that the original product was defective. Here the AI act plays an important role, because non-compliance with the standards set forth in the AI act, imply a lack of compliance with safety requirements. This in turn would trigger a presumption of defectiveness.

An important aspect of the updated PLD is the acknowledgment of an important trait of AI systems, namely that they often aren't static by nature and that multiple parties contribute to their development. For instance, if a deployer substantially modified an AI or a company integrated an AI component into a final product, that company is treated as a provider (hence as a producer for liability). [56] However, this is also considered in relation to defects based on developments of a AI-system that occur when a product is used by an end-user. Under the PLD a product is considered defective if it fails to provide the level of safety that the public is entitled to expect[57]. The directive acknowledges that consumers have a legitimate expectation that AI products will be designed in a way that limits the emergence of hazardous autonomous behaviour[58]. The ability to evolve autonomously is thus not treated as a neutral technical feature, but as a risk factor that producers are expected to anticipate and control.

That said, the "state of the art" defence remains available to producers[59]. This defence allows manufacturers to avoid liability if they can prove that the defect could not have been discovered given the scientific and technical knowledge available at the time the product was placed on the market. However, this defence is interpreted narrowly and will especially take into account the fulfilment of the standards set forth in the AI Act.

[54] Recital 9 AI Act.

[55] Hacker, *op. cit.,* note 23, p. 3.

[56] Montagnani *et al.*, *op. cit.*, note 4 , p. 11 f.

[57] Art. 7 PLD.

[58] Recitals 3, 30 PLD.

[59] Art. 11 para. 1 lit. e PLD.

## 3.1. ARTIFICIAL INTELLIGENCE LIABILITY DIRECTIVE

While the PLD has been passed and is currently in the process to be adopted by the member states, the same hasn't happened for the AILD. This directive hasn't been passed in its current form, amongst others because it could cause confusion within the AI legal framework, due to its potential overlap with the PLD[60]. Therefore, it will only be discussed briefly in the following text.

While the PLD is centered around the concept of a defective product, the Liability Directive proposal was based on fault based liability[61]. This means that in order for an injured party to have a right to claim compensation for damages, it is amongst others necessary to prove fault. This in turn usually requires the proof of a certain level of negligence or intent on the injuring party[62]. The duties set out in the AI Act could have served as objective standards of care for various actors when it comes to AILD related claims. If a provider or deployer violates an AI Act obligation and harm occurs, that violation will likely be compelling evidence in a negligence claim. This fault based regime could have been more appropriate both in order to support innovation, as well as to consider the role of the human operator who also has to show an adequate level of care[63]. However, the AILD proposal also contained additional mechanisms to protect injured parties. While the PLD only requires the defectiveness of a product, without fault, the AILD proposal contained mechanisms to ease the burden of proof through two mechanisms: injured parties have a right to compel evidence disclosure from AI system providers or users, and a rebuttable presumptions of causation in complex AI cases. In addition, if deployers fail to keep logs as required by the AI Act and the victim can't otherwise prove how the harm was caused, a court could have presumed a causal link between the AI's failure and the deployer's fault.

## 3.2. WORKPLACE RELATED EUROPEAN SAFETY STANDARDS

Safety standards in the workplace, similar to general AI safety standards set forth in the AI act do not regulate civil law claims for damages per se, but they will indirectly shape the framework of responsibilities and standards of care. Therefore it is important to mention European safety standards in regard to AI, as the

[60] Hacker, *op. cit.,* note 23, p. 6 f.

[61] Claudio, N. *et al.*, *Generative AI in EU law: Liability, privacy, intellectual property, and cybersecurity*, Computer Law & Security Review, Volume 55, 2024, p. 3.

[62] Hacker, *op. cit.,* note 23, p. 13.

[63] For a comprehensie review with further references see: Arcila, *op. cit.*, note 8, p. 6; European Commission, *op. cit.,* note 4, p. 33; Nissenbaum, H., *Accountability in a computerized society*, Science and engineering Ethics, Vol. 2, No. 1. p. 26.

deployment of AI systems in the workplace must also comply with the European Union's foundational framework for occupational safety and health, most notably the Framework Directive on Safety and Health of Workers ("OSH Framework Directive").[64] Employers are obliged to ensure the safety and health of workers in every aspect related to their work.[65] This duty is non-delegable and encompasses not only the physical environment but also the introduction of new work processes and tools, including digital and automated systems.[66] Employers must take necessary measures for the safety and health protection of workers, including prevention of occupational risks, provision of information and training, and the implementation of means to carry out these measures. It is within the responsibilities of employers to adapt to technical progress, give clear instructions and develop a coherent overall prevention policy that covers technology, organisation of work, working conditions, and social relationships.[67]

Moreover, the OSH Framework Directive requires worker consultation and participation, which includes the right of employees or their representatives to be informed and consulted on all matters affecting health and safety.[68] This obligation overlaps with Article 29 of the AI Act, which mandates information and consultation before the deployment of high-risk AI systems impacting workers. For example, introducing an AI system that monitors productivity or allocates tasks based on behavioural patterns would trigger both sets of obligations. Failure to consult workers in such scenarios could constitute a violation of both EU labour law and AI-specific regulatory requirements.

In addition, numerous sector specific sources have to be considered. For example, where AI systems are integrated into machinery or form part of intelligent robotic equipment, Directive 2006/42/EC on machinery requires that machines, including those with embedded AI components, comply with essential health and safety requirements. Similar rules apply in numerous other segments. Therefore, the AI Act has to be considered as part of the broader worker safety regulation.

[64] Council Directive of 12 June 1989 on the introduction of measures to encourage improvements in the safety and health of workers at work (89/391/EEC).

[65] Art. 5 para. 1 OSH Framework Directive.

[66] Art. 6 para. 1 OSH Framework Directive.

[67] Art. 6 para. 2 OSH Framework Directive.

[68] Art. 11 OSH Framework Directive.

## 4. RESPONSIBILITY DISTRIBUTION IN WORKPLACE ENVIRONMENTS: EMPLOYER OBLIGATIONS UNDER CROATIAN LAW

While the previous chapter has presented the obligations of various actors in the AI space under EU law, and through this established benchmarks for the duties of key parties, it is left to national law to determine the rights of injured parties to damages. Therefore, the following section outlines the general contractual damages regime in Croatia, and show how special rules governing liability allocation between employer and employee impact the obligations of employers.

In the following text we first discuss the legal relations between relevant parties and then consider two key constellations within the general requirements of a claim for damages: 1) cases in which an AI system used by the employer causes harm to the employee and 2) cases in which an AI system used by employees in work processes causes harm to a third party. While claims can exist based on a variety of grounds including contractual damages, torts, liability for dangerous activities or defective products etc.[69], we will limit our analysis to some key cases which best illustrate the role of the new AI framework in employment law, with the employer as central actor between AI system provider, employee and client[70]. In this context we will refer to the above mentioned examples of AI systems and look at the following constellations of contractual damages: damages caused by AI-operated heavy machinery to employees, damages caused by work-process optimization software to employees or third parties and damages caused by generative software as well as specialized diagnostic software to third parties.

### 4.1. THE INVOLVED PARTIES AND RESPECTIVE LIABILITY REGIMES

As stated above, the following analysis focuses on key constellations of liability distribution relevant to the employer's position in AI-integrated workplace environments. Three relational axes are of particular interest, namely: 1) between the employer and AI providers or distributors, 2) between the employer and third parties who may suffer harm and 3) between the employer and the employee.

[69] Perkušić, T., *Odgovornost za štete kod privremenog zapošljavanja*, Zbornik radova Pravnog fakulteta u Splitu, Vol. 58, 2/2021, pp. 633-655, p. 641 f.

[70] Even more complex cases could be presented with tort related obligations under Art. 1045 f. of the Croatian obligations act. However, for simplicity reasons, the authors focused on contract related claims which can be jointly presented in the following text.

In the first two constellations liability is typically governed by contractual arrangements and the general principles of fault-based liability under Croatian civil law. Between commercial parties or in relation to the employers clients, these obligations are usually determined through contracts, with liability arising in cases of non-performance or breach. In addition to this regime, various other relevant regimes exist like delict liability or liability for defective products. While these layers are legally relevant, a detailed treatment of strict product deficit liability and delict liability regimes falls outside the scope of this paper, which seeks to remain focused on employment-related implications and would otherwise require significantly broader analysis.

The relationship between employer and employee introduces additional complexity. On one hand, employers may be subject to strict liability for harm suffered by employees if such harm results from violations of workplace safety standards or the failure to provide adequate training, in line with the presented OSH standards. On the other hand, employees bear only limited liability towards their employer, and are generally liable for damages caused in the course of employment only in cases of gross negligence or intentional misconduct. This framework becomes particularly complex in cases where an employee, acting as part of the employment duties[71] or in relation to their employment relationship[72], causes harm to a third party, for example, by misusing or incorrectly operating an AI system in a way that leads to contractual damages. In such cases, the employer is liable based on presumed fault but can be exempted by proving that the employee acted with due care and in accordance with professional standards under the given circumstances.[73]

To examine these issues, the following analysis is structured according to the general requirements for contractual liability, with specific elements emphasized where relevant: (1) the existence of a breach of a contractual or statutory obligation arising from the employment relationship; (2) the occurrence of damage, whether material or non-material; (3) a causal link between the breach and the damage, assessed based on the principle of adequate causation and (4) the presence of fault on the part of the breaching party, unless the law provides otherwise, for example in the case of strict (objective) liability.[74]

[71] See on the position of the Supreme Court of the Republic of Croatia, VSRH, Revr – 986/17 from 11 July 2018.

[72] Vera, B. *et al.*, Veliki komentar novog Zakona o radu, Vaša knjiga, Zagreb, 2010, p. 153.

[73] Art. 1061 para. 1 Obligations Act.

[74] In detail about the development of these requirments see for example: Laleta, S., *Neka pitanja odgovornosti za štetu koju prouzroči posloprimac pri izvršavanju činidbe rada prema austrijskom pravu*, 1016 Zb. Prav. fak. Sveuč. Rij., 1991, Vol. 27, No. 2, pp. 1005-1031; Perkušić, T., *Zaštita i odgovornost za*

## 4.2. BREACH OF CONTRACT

Employers will usually enter into contractual relationships with AI providers or distributers in order to use AI systems. Thus contracts between Employers (in the role of AI deployers) on one side and AI providers or distributers will usually determine key aspects of their obligations. As mentioned above, actors like AI system providers cannot contractually transfer obligations that they have under the AI Act to other parties and through this relieve their responsibilities under the act itself. Commercial subjects are however free to distribute responsibilities on commercial law matters amongst themselves. Thus contractually agreeing on a higher burden on the operator under contract law is generally possible. However, such a transfer is limited by art. 345 para. 1 of the Croatian obligations act, which prevents contracting parties to exculpate a party in advance for gross negligence or intent. As the AI act clearly defines the legal obligations of a AI system provider, this standard cannot be decreased. However, contractually the obligations of the AI deployer can be increased in a manner that the deployer supports the fulfilment of the obligations of the AI provider, thus shifting part of the obligations to the deployer. For example, in the aforementioned case of AI-systems used to operate industrial robots, it is possible that the AI Provider agreed with the deployer to provide daily reports and ensure daily testing of the industrial robot. This standard could go beyond the minimum requirement in the AI Act for deployers, but a violation would shift at least part of the responsibility to the deployer.

Employers will furthermore have to enter into contractual relationships with employees.[75] Under Croatian employment law, including the integrated EU acquis, employers have numerous obligations, including the above already mentioned requirements to ensure employee safety, give clear instructions and adequate training.[76] Furthermore, employers are responsible for damages under general civil law principles towards their employees[77], while employees have an *ex lege* limitation only for gross negligence and intent.[78] Thus, in cases where an employee doesn't operate an AI-system in line with provided standards, and this causes damages, it would have to be established both under domestic employment law and the AI act, if the employee has sufficiently been trained for the use of the system, and even if this was the case, if he acted grossly negligent. It is thus clear that in cases

*štetu od mobinga na radu i u vezi s radom*, Zbornik Pravnog fakulteta Sveučilišta u Rijeci, Vol. 42, No. 3, 2021, pp. 853-872.

[75] Art. 10 para. 1 Croatian Employment Act, Offical Gazette No. 93/14, 127/17, 98/19, 151/22, 46/23, 64/23.

[76] Art 3 f. Croatian Workplace safety act, Offical Gazette No. 71/14, 118/14, 154/14, 94/18, 96/18.

[77] Art. 111 Croatian Employment Act.

[78] Art. 107 Croatian Employment Act.

where damages to an employee are caused by autonomous robots, autonomous vehicles or other comparable machinery, the employee will usually have a claim against the employer directly. The EU legal framework here is much more relevant for the recourse rights of the employer to the manufacturer or seller of the defective technology.[79] Simultaneously, the employer is not able extent the contractual obligations of their employees in a comparable manner to what AI providers or distributers can through commercial contracts with them.

In this context, it can furthermore be considered what constitutes a breach of contract. In general this is non-fulfilment of an obligation or sub-par fulfilment. However, especially when it comes to AI-systems, it is important to consider the benchmark of fulfilment. A good example of this are AI systems that outperform humans. Some AI systems can exhibit performance beyond human capabilities and thus show significantly superior results to average comparable individuals (average individuals acting with reasonable care or experts acting with expert knowledge and care in a specific field). Here, the assessment benchmark first needs to be established, as an AI-system in this case should not be assessed against human capabilities alone, nor should their exceptional output automatically exempt AI system providers or deployers from liability. The mere fact that an AI performs beyond typical human standards does not justify lowering safety or accountability thresholds. For example, a medical diagnostic tool that significantly outperforms medical professionals in lung cancer diagnosis, cannot simply be considered to be working properly just because it has a higher accuracy rate than medical experts. This is only logical, as many tools and software solutions have served to improve on human behaviour, and have set new standards. For example, the standard for functioning telecommunications isn't the distance that humans can naturally communicate, and the standard for a search engine isn't how fast an individual can conduct library research on a topic.

At the same time, setting the industry's top-performing system as the baseline for non-defectiveness would create unrealistic expectations and discourage healthy competition, potentially leading to market concentration and innovation stagnation. Instead, some authors propose that the evaluation of such systems should be based on principled criteria: whether the system's design reflects a reasonable balance of risks and benefits, whether it serves a legitimate and socially beneficial purpose, and whether users are properly informed about any unavoidable limitations or risks. This

[79] Andrea, B., *Artificial Intelligence and Civil Liability, Study for the Policy Department for Citizens' Rights and Constitutional Affairs*, Directorate-General for Internal Policies, PE 621.926 - July 2020, p. 105, available at:
[https://www.europarl.europa.eu/RegData/etudes/STUD/2020/621926/IPOL_STU(2020)621926_EN.pdf], Accessed 1 April 2025.

ensures that technological excellence does not come at the expense of user protection or legal clarity, while still promoting ongoing innovation in high-performance AI.[80]

## 4.3. DAMAGE

While AI Systems become increasingly advanced and simultaneously more beneficial for commercial use, many employers still avoid implementing more complex AI systems. Liability for damages caused by AI systems are considered one of the key reasons why corporations avoid implementing these technologies[81]. In relation to contractual damages, the general principle is that the creditor is entitled to compensation for ordinary damage and loss of profit, as well as equitable compensation for non-material damage, which the debtor must have foreseen at the time of the conclusion of the contract as possible consequences of the breach of contract, considering the facts that were known or ought to have been known to him at that time[82]. For example, in relation to logistics software, the AI system provider must have been aware that a fault in the system can cause delays to third parties and thus damage production chains. However, if the system hasn't had a component that grades employee performance and the employer hasn't notified the provider of planned changes or integrations to the system, the system provider could not have expected potential damages to employees caused by these systems. In contrast, AI systems that are initially categorized as high-risk imply a broader understanding of expected risks. So for example an AI provider will have to consider in advance all types of potential damages that can be caused in relation to medical diagnostics AI or heavy machinery.

## 4.4. CAUSAL LINK

The public consultation preceding proposals for the regulations on AI liability has shown that there is a strong support for harmonization in this area. Specific issues that were raised were challenges concerning the burden of proof and access to information important to assess the role of AI in causing damages, as well as the relationship between clear compensation rights and trust in the use of AI[83].

[80] Hacker, *op. cit.,* note 23, p. 17.

[81] European Commission, Directorate-General for Communications Networks, Content, and Technology, European enterprise survey on the use of technologies based on artificial intelligence: final report, Publications Office, 2020. The survey refers to the broader category of natural language processing models, p. 71 f.

[82] Art. 346 para. 1 ZOO.

[83] European Commission, Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs (DGGROW)Directorate-General for Justice and Consumers (DG JUST): Adapting Civil Lia-

In general, it is necessary to prove that a contract violation has caused damages. In practice, this can be very challenging concerning AI systems which are adaptable, continuously developing and often highly complex[84]. A causal link under the *condition sine qua non* principle can be established both with the developer as well as the operator of an AI-system. For example, faulty inputs of an operator that affected the machine learning process of an AI-system of an industrial robot, can impact the actions of a robot which in turn can cause serious damage.[85] Here the question would be if the provider has given clear instructions and established sufficient safety mechanisms and if the deployer has followed these instructions. It would furthermore have to be considered to what extent the employer as deployer of the AI has conducted sufficient training and given clear instructions towards the employees as natural persons who work with the AI system. While these considerations are already complex, it has also to be considered that AI-systems will increasingly be integrated with other systems, including various other AI-systems, which will only make it more difficult to identify the cause of a harmful event.[86]

The responsibility of commercial users of AI driven robots towards their employees is strongly influenced through the employers obligations under worker protection laws in the EU and member states[87]. While the AI directive aims primarily at the AI System provider, actually a majority of the risks concerning the use of new technologies will likely contractually be shifted towards the employer. Further-

bility Rules to the Digital Age and Artificial Intelligence - Factual summary report on public consultation, Ref. Ares (2022)2620305 - 06/04/2022, p. 7 f. Available at: [https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Civil-liability-adapting-liability-rules-to-the-digital-age-and-artificial-intelligence/public-consultation_en], Accessed 1 April 2025.

[84] European Commission, *op. cit.*, note 4. p. 20.

[85] See Cauffman, C., *Robo-liability: The European Union in search of the best way to deal with liability for damage caused by artificial intelligence*, Maastricht Journal of European and Comparative Law, Vol. 25, No. 5, 2018, pp. 527-532.

[86] European Commission, *op. cit.*, note 4, p. 22.

[87] Bertolini, *op. cit.*, note 82, p. 104 with further references: 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, OJ L 157, 9 June 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, 30 December1989; (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 Directiv 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, 30 December 1989.

more, employers will have to cover most damages caused in relation to mistakes made by their employees. Studies have shown that with AI based systems and robots becoming more autonomous, the blame for errors is shifted towards them instead of the co-worker operating them[88]. Especially when considering special worker protection regulation in the EU and the particular liability distribution between employer and employee, it is valid to question whether current civil law is fit to regulate work accidents related to AI.[89] A helpful aspect in this regard is already existing legislation on specific AI related systems. For example, Germany has determined that a driver up to autonomy level 4 is responsible to supervise the driving task and resume control when this is required. If the driver does not act under these rules, an accident would usually be considered human error. In the case that an accident still occurred, even though the driver did not violate his obligations, the liability would fall to the owner, while it would be questionable against whom in the value-chain of the self-driving car the owner would have potential recourse claims.[90]

Furthermore, AI transparency is a topic that is central to the consideration of liability distribution amongst all parties in workplace related accidents[91]. In order to determine whether an accident was the result of human error, a mistake in the AI or an unforeseen event, it will often be necessary to analyse the decision-making process of the AI[92]. This can be complex in many cases of complex products, or expert products like diagnostic software. This is especially the case if the AI is provided by third parties through a business model like artificial intelligence as a service (AIaaS) where the creator of the AI holds all intellectual property rights and will not be inclined to share confident data on the AI model or data set with other parties.[93] It is especially problematic, that AIaaS can regularly be updated and thus previously reliable AI solutions might contain errors and thus cause dam-

[88] Furlough, C.; Stokes, T.; Gillan D. J., *Attributing Blame to Robots: I The Influence of Robot Autonomy,* Human Factors, 2019.

[89] Taes, S., *Robotisation and Labour Law: The Dark Factory: the Dark Side of Work?* in Artificial Intelligence and the Law, Intersentia, 2021; Study of the European Parliamentary Research Service, Panel for the Future of Science and Technology: AI and digital tools in workplace management and evaluation An assessment of the EU's legal framework, PE 729.516 – May 2022 EN, p. 5, available at: [https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729516/EPRS_STU(2022)729516_EN.pdf], Accessed 1 April 2025.

[90] Bertolini, *op. cit.,* note 82, p. 109.

[91] Matthews, J., *Patterns and Antipatterns, Principles, and Pitfalls: Accountability and Transparency in Artificial Intelligence*, AI Magazine, 2020, p. 86 f.

[92] European Parliament, "Resolution with recommendations to the Commission on a civil liability regime for artificial intelligence", Brussels, 20 October 2020. 2020/2014(INL), p. 6, available at: [https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_EN.html], Accessed 1 April 2025.

[93] European Parliamentary Research Service, *op. cit.*, note 92.

ages.[94] While the data collection requirements under the AI act will be helpful to ensure that adequate data exists on deployer and provider levels, the extent to which such data will be provided in civil procedures to the counter party, will have to be determined in practice, based on the legitimate interests to protect business secrets and the obligation to provide transparent services and defend the position under contractual damages.

For purposes of comparison, it makes sense to mention the AILD in this context. The AILD would have created a presumption of casual link in cases where a violation of the obligations of the AI act can be proven and a reasonable case can be made for causation under tort law.[95] Under the AILD the injured party would have only hade to provide plausible evidence related to damages caused by a high-risk AI system, while the respective actor would have had to disclose relevant information that can contribute to the proof of damages and causation. In case that such information is not provided, this would constitute a rebuttable presumption of a breach of duty of care.[96]

## 4.5 FAULT

To which level fault has to be determined depends on the type of contractual relationship. Under Croatian contract liability law, the injured party usually only has to prove a breach of contract, while ordinary negligence is assumed and for most cases sufficient to represent a valid basis for a claim for damages. The debtor can be released from liability for damages if they prove that they could not fulfil their obligation, or that the delay in fulfilment was due to external, extraordinary, and unforeseeable circumstances arising after the conclusion of the contract, which they could not have prevented, eliminated, or avoided.[97] This general principle has wide reaching consequences when employees cause harm due to their actions. As already mentioned above, employers bear the commercial risk of their activities[98] and thus employees are only liable in cases of their gross negligence. However, as

[94] Study of the European Parliamentary Research Service, Panel for the Future of Science and Technology: AI and digital tools in workplace management and evaluation An assessment of the EU's legal framework, PE 729.516 – May 2022 EN, p. 32, available at: [https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729516/EPRS_STU(2022)729516_ EN.pdf], Accessed 1 April 2025.

[95] Tambiama, M., *Artificial Intelligence Liability Directive*, European Parliamentary Research Service, PE 739.342 (Feb. 2023), available at: [https://courses.ilac.eu/wp-content/uploads/2023/03/AI-DIRECTIVE.pdf], Accessed: 1 April 2025.

[96] Novelli *et al.*, *op. cit.*, note 62, p. 2.

[97] Art. 343 Croatian obligations act.

[98] Supreme Court of the Republic of Croatia - VSRH, Revr – 150/17 from 3 July 2019.

only ordinary negligence is assumed on the side of the party that caused damages, employers do not just have to prove a breach of contract when harm to them or to third parties is caused by employees. In order to have a claim for damages or regress against their employees[99], they must prove the specific level of gross negligence on part of their employees.[100]

Furthermore, in relation between employer and AI system provider, it can be complex to prove who is at fault. This prof becomes even more complex if an AI system damaged a third party. For example, a generative AI system created a deep fake based on available images provided by an employee. It could be questionable, if the AI system didn't have enough safeguards in place or the instructions to deployers were unclear (fault of deployer), if the instructions were not clearly communicated to the employee, or the employee wasn't sufficiently trained to use the system (fault of the employer/deployer), or the employee disregarded safety standards in order to simplify the completion of a task, and used unauthorized images of clients (fault of the employee due to gross negligence or intent).[101]

In general, it is likely that the employer will be in a difficult spot due to their obligation to compensate for damages for incorrect use of AI systems by their employees, strict contractual obligations through which AI system providers and distributers will try to protect themselves, and the protected position of employees. Not just that employers have the obligation to provide adequate training and instructions on often very complex systems[102], employee liability is also limited to gross negligence and intent, which is particularily important in connection to AI systems for numerous reasons. On one hand, automation bias causes users to over-rely on systems even when they are incorrect; on the other, algorithmic aversion leads users to distrust accurate systems and override them unnecessarily. These conflicting tendencies, combined with reduced vigilance and insufficiently designed interfaces or oversight, make it difficult to ensure effective collaboration between operator and AI.[103]

Furthermore, these issues will only be more intense in highly complex environments. Especially in the field of diagnostic software and medical devices, human

[99] Tintić, N., *Radno i socijalno pravo, knjiga prva: Radni odnosi (I)*, Narodne novine, p. 658.

[100] See for example Supreme Court of the Republic of Croatia, Revr – 1504/16 od 15 May 2018.

[101] Gross negligence of employees under Croatian law requires a clear breach of duty like the insuficient fulfilment of a duty within the description of their position, see Supreme Court of the Republic of Croatia VSRH, Rev – 834/05 from 5 October 2005.

[102] Bertolini, *op. cit.,* note 82, p. 105.

[103] For a comprehensie review with further references see: Arcila, *op. cit.,* note 8, p. 4.

oversight plays a crucial role.[104] An important distinction is weather AI based solutions support the medical practitioner or are able to operate autonomously. If an error occurs with a fully autonomous system, this would point to a liability of the manufacturer, but it is unlikely that such fully automated systems will be integrated soon.[105] It is much more likely that AI will serve as support for medical practitioners. Medical practitioners will thus be in a difficult position in cases where AI provides a diagnosis or proposes a procedure that has a very high likelihood of being accurate, but is still under 100%. In these cases, it is questionable to what extent a medical practitioner would be liable if he decides to accept the AI suggestion without additional tests, but it turns out to be false, or in the opposite situation decides against it, but his decision turns out to be false.[106] Simply conducting numerous additional tests as if there was no AI suggestion is however not a universal solution for this problem, as this is time consuming, resource intensive and would directly contradict the purpose of the AI system. Specialized and expert areas like medicine or law will in particular rely on sector specific standards in order to determine how to operate AI-systems.[107] Thus it will require adequate standards guided by current medical best practices.[108] In conclusion, it can thus be expected that AI implementation will require an increase in new working standards, particularly in more specialized fields.

## 5. CONCLUSIONS

The integration of AI systems into the workplace presents a complex legal landscape, which is especially challenging for employers who often find themselves at the crossroads of competing obligations. The EU's AI Act, the updated PLD, as well as the proposed AILD aim to establish a coherent regulatory framework. However, especially due to the abandoning of the AILD significant gaps remain, particularly in the realm of civil liability within employment contexts.

Employers, as AI deployers, have significant responsibilities under the AI Act, including compliance with safety standards, ensuring proper oversight, and safeguarding employee rights. At the same time, it can be expected that commercial contracts with AI providers will often shift an additional burden onto employers by imposing heightened obligations and indirectly limiting the provider's own li-

[104] Onitiu, D., *The limits of explainability & human oversight in the EU Commission's proposal for the regulation on AI—a critical approach focusing on medical diagnostic systems*, *Inf Commun Technol Law*, 2023, Vol. 32, No. 2, pp. 170–188.

[105] Bertolini, *op. cit.*, note 82, p. 111.

[106] Bertolini, *op. cit.*, note 82, p. 113.

[107] Onitiu, *op. cit.,* note 105, p. 187 f.

[108] Bertolini, *op. cit.*, note 82, p. 113.

ability. These agreements, while sometimes permissible under commercial law, risk placing the employer in a disproportionately vulnerable legal position, especially given that providers retain intellectual property rights and may have a better overview over data relevant to assess liability early.

Simultaneously, employers must fulfil their duties to employees under national labour laws and EU workplace safety directives, which mandate safe working conditions, adequate training, and clear communication regarding new technologies. This duty of care is not mitigated by the increasing autonomy of AI systems; instead, it intensifies the employer's role as both operator and intermediary between the provider and the employee. Furthermore, while employers can potentially seek redress from AI providers or distributors, they are often the first point of liability.

This triangulated legal pressure, between contractual liability to providers, regulatory obligations to employees, and civil liability towards third parties, places employers in a uniquely precarious legal position. They are expected to manage AI systems they may not fully control or understand while ensuring both technical compliance and human safety.

Given this complexity, it can be expected that there will be a growing emphasis on developing clear best practices and technical standards, particularly in highly complex fields and areas where serious damages can occur. Such standards are essential not only for ensuring safe AI deployment but also for enhancing legal certainty. For employers in particular, these evolving norms will be crucial in helping to delineate reasonable expectations, clarify liability boundaries, and foster trust in AI technologies within the workplace.

## REFERENCES

### BOOKS AND ARTICLES

1. Babić, V.; Crnić, I.; Cvitanović, I.; Gotovac, V.; Gašpar Lukić, M.; Milković, D.; Tadić, I., Zuber, M.; Žic, I., Veliki komentar novog Zakona o radu, Vaša knjiga, Zagreb 2010.
2. Arcila, B. B., *AI liability in Europe: How does it complement risk regulation and deal with the problem of human oversight?*, Computer Law & Security Review, Volume 54, 2024
3. Cauffman, C., *Robo-liability: The European Union in search of the best way to deal with liability for damage caused by artificial intelligence*, Maastricht Journal of European and Comparative Law, Vol. 25, No. 5, 2018, pp. 527–532.
4. Ebers, M.; Hoch, V.; Rosenkranz, F.; Ruschemeier, H.; Steinrötter B, *The European Commission's Proposal for an Artificial Intelligence Act— A Critical Assessment by Members of the Robotics And Ai Law Society* (RAILS), J 4, No. 4, 2021, pp. 589–603.
5. Furlough, C.; Stokes, T.; Gillan D. J., *Attributing Blame to Robots: I The Influence of Robot Autonomy,* Human Factors, 2019.

6. Hacker, P.; Philipp, H., T*he European AI liability directives – Critique of a half-hearted approach and lessons for the future*, Computer Law & Security Review, Volume 51, 2023
7. Matthews, J., *Patterns and Antipatterns, Principles, and Pitfalls: Accountability and Transparency in Artificial Intelligence*, AI Magazine, 2020
8. Montagnani, M. L.; Najjar, M. C.; Davola, A., *The EU Regulatory approach(es) to AI liability, and its Application to the financial services market*, Computer Law & Security Review, Volume 53, 2024
9. Nissenbaum, H., *Accountability in a computerized society*, Science and engineering Ethics, Vol. 2, No. 1.
10. Novelli, C.; Casolari, F.; Hacker, P.; Spedicato, G.; Floridi, L., *Generative AI in EU law: Liability, privacy, intellectual property, and cybersecurity*, Computer Law & Security Review, Volume 55, 2024., pp. 1–16.
11. Onitiu, D., *The limits of explainability & human oversight in the EU Commission's proposal for the regulation on AI—a critical approach focusing on medical diagnostic systems*, *Inf Commun Technol Law*, 2023, Vol. 32, No. 2, pp. 170–188.
12. Perkušić, T., *Odgovornost za štete kod privremenog zapošljavanja*, Zbornik radova Pravnog fakulteta u Splitu, god. 58, 2/2021, pp. 633-655.
13. Perkušić, T., *Zaštita i odgovornost za štetu od mobinga na radu i u vezi s radom*, Zbornik Pravnog fakulteta Sveučilišta u Rijeci, Vol. 42, No. 3, 2021, pp. 853-872.
14. Laleta, S., *Neka pitanja odgovornosti za štetu koju prouzroči posloprimac pri izvršavanju činidbe rada prema austrijskom pravu*, 1016 Zb. Prav. fak. Sveuč. Rij., 1991, Vol. 27, No. 2, pp. 1005-1031.
15. Taes, S., *Robotisation and Labour Law: The Dark Factory: the Dark Side of Work?* in Artificial Intelligence and the Law, Intersentia, 2021
16. Tintić, N., *Radno i socijalno pravo, knjiga prva: Radni odnosi (I)*, Narodne novine, 1969.

## REGULATIONS AND DOCUMENTS

1. Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM(2021) 206 final, Brussels, 21 April 2021
2. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013 and (EU) No 168/2013 (Artificial Intelligence Act) [2024] OJ L168/1
3. Directive 2002/14/EC of the European Parliament and of the Council of 11 March 2002 establishing a general framework for informing and consulting employees in the European Community [2002] OJ L80/29
4. Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products (recast) [2024] OJ L[vol]/2024/2853
5. 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 (General Data Protection Regulation) [2016] OJ L119/1

6. Directive 2014/104/EU of the European Parliament and of the Council of 26 November 2014 on certain rules governing actions for damages under national law for infringements of the competition law provisions of the Member States and of the European Union [2014] OJ L349/1
7. 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 [1989] OJ L183/1
8. Zakon o radu [Croatian Employment Act], Narodne novine, No. 93/14, 127/17, 98/19, 151/22, 46/23, 64/23
9. Zakon o zaštiti na radu [Croatian Workplace Safety Act], Narodne novine, No. 71/14, 118/14, 154/14, 94/18, 96/18
10. Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC [2006] OJ L157/24
11. 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 [2016] OJ L81/51
12. Council Directive 89/686/EEC of 21 December 1989 on the approximation of the laws of the Member States relating to personal protective equipment [1989] OJ L399/18
13. 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 within the meaning of Article 16(1) of Directive 89/391/EEC) [2009] OJ L260/5
14. 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) [1989] OJ L393/1
15. European Parliament, Resolution with recommendations to the Commission on a civil liability regime for artificial intelligence, 2020/2014(INL), 20 October 2020, 6 https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_EN.html [accessed 1 April 2025]

## JUDGMENTS AND OTHER DECISIONS

1. Supreme Court of the Republic of Croatia (VSRH) Revr 150/17, 3 July 2019
2. Supreme Court of the Republic of Croatia (VSRH) Rev 834/05, 5 October 2005
3. Supreme Court of the Republic of Croatia (VSRH) Revr 986/17, 11 July 2018
4. López Ribalda and Others v Spain [2019] ECHR 752, Applications Nos 1874/13 and 8567/13 (GC, 17 October 2019)

## INTERNET SOURCES

1. Andrea Bertolini, *Artificial Intelligence and Civil Liability*, Study for the Policy Department for Citizens' Rights and Constitutional Affairs, DG Internal Policies, PE621.926 (European Parliament, July 2020) , available at:
[https://www.europarl.europa.eu/RegData/etudes/STUD/2020/621926/IPOL_STU(2020)621926_EN.pdf], Accessed 1 April 2025.

2. European Commission, *Adapting Civil Liability Rules to the Digital Age and Artificial Intelligence – Factual Summary Report on Public Consultation*, Ref Ares(2022)2620305 (Publications Office, 2022), available at: [https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Civil-liability-adapting-liability-rules-to-the-digital-age-and-artificial-intelligence/public-consultation_en], Accessed 1 April 2025.
3. European Parliament, *Artificial intelligence: threats and opportunities* (2020) [https://www.europarl.europa.eu/topics/en/article/20200918STO87404/artificial-intelligence-threats-and-opportunities], Accessed 1 April 2025.
4. European Commission, *Liability for Artificial Intelligence and Other Emerging Digital Technologies* (Publications Office, 2019) 20 [https://data.europa.eu/doi/10.2838/573689], Accessed 1 April 2025.
5. European Parliamentary Research Service, *AI and Digital Tools in Workplace Management and Evaluation: An Assessment of the EU's Legal Framework*, PE729.516 (Panel for the Future of Science and Technology, 2022), available at: [https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729516/EPRS_STU(2022)729516_EN.pdf], Accessed 1 April 2025.
6. Tibor Madiega, *'Artificial Intelligence Liability Directive'*, PE739.342 (European Parliamentary Research Service, February 2023), available at:

   [https://courses.ilac.eu/wp-content/uploads/2023/03/AI-DIRECTIVE.pdf], Accessed 1 April 2025