MOKSLO TAIKOMIEJI TYRIMAI, 2025 Nr. 21 (2), p. 40-47
eISSN 3030-1823; DOI: https://doi.org/10.59476/mtt2025.v2i21.730 / http://ojs.kaunokolegija.lt/index.php/mttlk/index

HUMAN-CENTRED ROBOTICS AND THE EU AI ACT: SELECTED STANDARDS AND IMPLICATIONS

Ralf Roßkopf

Technical University of Applied Sciences Würzburg-Schweinfurt

Abstract. Robotics and AI are key factors in enhancing business and national resilience, particularly in maintaining high-wage manufacturing in countries facing demographic challenges. Both are instrumental in making manufacturing more agile and flexible. Robots and humans will have to collaborate closely. Creating the necessary intelligent autonomous systems will go well beyond the typical considerations of machine learning. In line with the EU's Industry 5.0 vision for a sustainable, human-centred and resilient European industry, humans and robots are expected to work so closely together that robot software must be designed with humans in mind from the outset. Thus, ethical, legal, and social implications (ELSI) must also be considered. Legal implications are multifaceted, ranging from AI Law, Product Liability Law, Product Safety Law, Machinery Law, to Technical Standards, Data Protection Law, Copyright and IP Law, Labour Law, etc. This contribution will briefly introduce the required technical features and, based on that, explore selected relevant legal implications and related standards of the new EU AI Act. The Act aims to promote human-centricity and entered into force on 1 August 2024, with its applicability phased in over a period of three years until 2 August 2027. Special references will be made to human-centredness, the subsumption of the plant owner to the categories of obligated parties (provider, product manufacturer, deployer, authorised representative or distributor), as well as the classification to the AI risk scheme (prohibited risks, high risks, transparency risks, general-purpose risks, and systemic risks as well as minimal risks) and related obligations. The high relevance of the AI Act for industrial human-robot settings will be shown. As AI evolves exponentially, so does its significance for industrial and national agility and resilience. Obligations vary widely according to risk classification and the obligated operator. Coordination and information flows between providers and deployers of related AI systems are key. As plant owners might become providers themselves, the duties could be more varied than initially assumed. Design and implementation of human-centred robotic scenarios, thus, should be well planned, structured, documented, and constantly evaluated. The respective AI models and AI systems need to be legally compliant and human-centred by design. An unprecedented dialogue across disciplinary fields is required.

Keywords: AI Act, robot, industry, human, risk, obligation, law

Introduction

Against the backdrop of new geopolitical lines of military, political, and trade conflicts, business, industrial, and national resilience become existential. In many European countries, this resilience is threatened from within by population decline and cumbersome structures. The European Union's vision of Industry 5.0 views adaptable production capacity as a core element for the needed resilience (Breque et al., 2021, p. 14). Robotics and AI can be key factors for maintaining industrial sites in demographically endangered high-wage countries, especially for more agile and flexible production. They can strengthen resilience by leveraging autonomous production impacts and improving productivity (Lin, Lukodono, 2025). In many cases, such more agile production is only possible through close cooperation between robots and humans. It is also necessary for creating, enabling, and realizing a smartly integrated and highly dynamic industrial environment.

Creating the necessary intelligent autonomous systems will go well beyond the typical considerations of machine learning (ML), as it often neglects changes in the operating conditions from training to runtime, as well as the safety-critical nature of robot actions during both. Robots are physically constrained systems embodied in space and time. To navigate in their environments or manipulate objects, they rely on an internal model of the world in which they operate (Kroemer et al., 2022). Traditionally, the model is constructed and tuned for a specific task the robot has to tackle (Wulfmeier et al., 2021). This is not sustainable in dynamically evolving industrial environments, where the robot has to adapt to gradually changing conditions, while, at the same time, not losing the ability to perform previously learned tasks. This requires techniques of continual (lifelong) learning (Ramapuram et al., 2020) of a unified representation of the robot environments suitable for robotics mobility, sensing, and manipulation that takes into account the relational nature of the robots' interaction with the environment, i.e., with objects and agents. Novel Machine Learning (ML) methods are required that focus on decentralized distributed learning (DDL). Existing research on learning under varying conditions is categorized as lifelong, transfer, or few-shot learning. A combination of these concepts, supported by modern deep representation learning, is needed. In line with the EU's Industry 5.0 vision, humans and robots are expected to work so closely together that robot software must inevitably be designed with humans in mind from the outset. A critical point in this context is the question of safety (Brunke et al., 2022): Learning

methods for controlling robots while they navigate or manipulate objects must consider that the robots should not constitute any excessive danger for humans in the human-robot teams. Constraints must be imposed on the admissible robot dynamics, which must be classified into different categories.

Human-centredness is still subject to discourse. Literature on the topic is characterized by overlaps and diversity. Having reviewed existing proposals, Schmager et al. (2025, p. 6) outline a new definition:

> "Human-Centered AI (HCAI) focuses on understanding purposes, human values, and desired AI properties in the creation of AI systems by applying Human Centered Design practices. HCAI seeks to augment human capabilities while maintaining human control over AI systems, by considering the necessity, context, and ethical and legal conditions of the AI system as well as promoting individual and societal well-being."

One might want to add performance, at least for the industrial environment. Conceptual frameworks for task performance analysis of human-robot interaction, however, are just emerging. Relevant identified human-centred factors are trust, safety, acceptance, user motivation, satisfaction, perceived support, and ergonomics, while system-centred factors are reliability, autonomy, and adaptiveness (Pasquale et al., 2024). Thus, ethical, legal, and social implications (ELSI) must be considered, such as human colleagues' expectations of robots, and how trust and traceability can be achieved when humans and robots collaborate at work. Numerous human (e.g., comprehensibility, trustworthiness) and legal requirements (e.g., liability, data security) must be met. People's experience, interpretation, and interaction with a learning robot – e.g., as (un)trustworthy, (im)predictable, (un)helpful, as a counterpart or a tool – are central (Sanfillippo et al., 2025). Explainability, traceability, and trust are key (Donath, 2020). Setting up human-robot teams and the related process planning have to integrate these technical and ELSI aspects. Both rely on AI in terms of safe learning and representation learning. To outline specifically the legal framework for ELSI-integrated human-robotics for industrial environments, lawyers have to explore new grounds. Recognizing the relevance of AI for human-centred robotics, the most significant is the European Union's new Regulation 2024/1689 of 13 June 2024, laying down harmonised rules on artificial intelligence (Artificial Intelligence Act – AI Act). The objective of the following legal analysis is to deliver a basic understanding of this new legal artwork, to give a first overview of related legal implications, and to identify as well as analyse legal standards relevant for human-centred robotics.

The AI Act

The AI Act entered into force on 1 August 2024. While prohibitions, definitions, and the provision of AI literacy are applicable already since 2 February 2025, the rules on governance and general-purpose AI will be applicable from 2 August 2025, and regulations on AI systems classified as high-risk for their embeddedness in regulated products (Art. 6(1) Annex I AI Act) as late as 2 August 2027. The applicability of the main body of regulations, including any other high-risk AI system (Art. 6(2) Annex III AI Act), is set for 2 August 2026 (Art. 113 AI Act). The idea of human-centred robotics is fully compliant with the purpose of the AI Act and in line with the EU's vision of Industry 5.0, "going beyond producing goods and services for profit" but serving instead a "wider purpose" that "constitutes three core elements: human-centricity, sustainability and resilience" (Breque et al., 2021, p. 13).

> "[A] human-centric approach in industry puts core human needs and interests at the heart of the production process. Rather than asking what we can do with new technology, we ask what the technology can do for us. Rather than asking the industry worker to adapt his or her skills to the needs of rapidly evolving technology, we want to use technology to adapt the production process to the needs of the worker, e.g., to guide and train him/her. It also means making sure the use of new technologies does not impinge on workers' fundamental rights, such as the right to privacy, autonomy, and human dignity" (Breque et al., 2021, p. 14).

Accordingly, Art. 1(1) AI-Act more generally defines its purpose as

> "to improve the functioning of the internal market and promote the uptake of human-centric and trustworthy artificial intelligence (AI), while ensuring a high level of protection of health, safety, fundamental rights enshrined in the Charter, including democracy, the rule of law and environmental protection, against the harmful effects of AI systems in the Union and supporting innovation."

These objectives are similarly highlighted in different recitals (Recital 1, 6, 8, 27, 176). AI is normatively seen as a "tool for people, with the ultimate aim of increasing human well-being" (Recital 6) and to serve people, to respect human dignity and personal autonomy, as well as to remain under the control and oversight

of humans (Recital 27). Human-centeredness is meant to mitigate the risks and possible material or immaterial harm to public interests and fundamental rights, including physical, societal, and economic harm. The risk itself is defined as "the combination of the probability of an occurrence of harm and the severity of that harm" (Art. 3(2) AI Act). In the context of AI-based industrial robotics, possible damage specifically concerns the physical and mental integrity of human "work colleagues" and the handling of information obtained. The AI Act introduces a classification of AI risks as unacceptable (prohibited AI practices, Art. 5 AI Act), high (high-risk AI systems, Art. 6-49 AI Act), transparency related (certain AI systems, Art. 50 AI Act), general-purpose and systemic (general-purpose AI models, Art. 51-56 AI Act) and minimal (EC, 2024). The latter are the majority. Obligations vary according to the risk categorisation. Obligations for different risk categories might apply in parallel if all conditions are met. Violations are penalized and fined (Art. 99-101 AI Act).

The Obligated Parties

Obligations vary according to the personal categorisation of operators, i.e., provider, product manufacturer, deployer, authorised representative, importer, or distributor (Art. 3 No. 8 AI Act). More than one attribute might apply to one person or body (Wendehorst, 2024a). The most relevant in our context are the provider and the deployer. The deployer is described as "a 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" (Art. 3(4) AI Act). Obligations for the deployer are far more limited than for the provider and concern AI literacy (Art. 4 AI Act), obligations specifically concerning high-risk AI systems (Art. 26 AI Act), fundamental rights impact assessment (Art. 27 AI Act), registration (Art. 49(3) AI Act), transparency in case of emotion recognition systems (Art. 3(39) AI Act), biometrical categorisation systems, deep fakes (Art. 3(60) AI Act) and manipulation of text purposed for informing the public on matters of public interest (Art. 50(3)-(4) AI Act), listing of data into the EU data base (Art. 71(3) AI Act) and explanation of individual decision-making (Art. 86(1) AI Act). A plant owner, running AI-driven robots, is typically seen as a deployer. In many instances, though, he or she additionally is to be regarded as a provider, namely.

> "a natural or legal person, public authority, agency or other body 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" (Art. 3 No. 3 AI Act).

'Placing on the market' "means the first making available of an AI system or a general-purpose AI model on the Union market" (Art. 3 No. 9 AI Act). 'Putting into service' "means the supply of an AI system for first use directly to the deployer or for own use in the Union for its intended purpose" (Art. 3 No. 11 AI Act), while the "intended purpose" is defined as

> "the use for which an AI system is intended by the provider, including the specific context and conditions for use, as specified in the information supplied by the provider in the instructions for use, promotional or sales materials, as well as in the technical documentation" (Art. 3 No. 12 AI Act).

Anyone who develops or commissions the development of an individual AI system to then transfer it directly to the deployer or to use it solely in their own organisation and domain for their own purposes is subject to the same obligations as those who place an AI system on the market (Wendehorst, 2024a). This might be very relevant with respect to the diversity of industrial settings and requirements where human-centred robots are supposed to be integrated. The relevance is increased by the possible extension of the term 'provider' to any distributor, importer, deployer or other third party if they put their name or trademark on an AI system, make substantial modification (Art. 3(23) AI Act) to it or modify the intended purpose of it (Art. 25(1) (a-c) AI Act). Though by wording and systematic, this provision only applies to high-risk systems, it is discussed already, whether the extension needs to be applied accordingly to AI systems triggering transparency obligations (Art. 50 AI Act) and general-purpose AI models (Art. 53 ff. AI Act) (Wendehorst, 2024). Another extension of the attribute 'provider' is owed to Art. 25(3) AI Act in the case of high-risk AI systems that are safety components of products covered by Annex I Section A AI Act and, therefore, regarded as high-risk AI systems (Art. 6(1) AI Act). The product manufacturer shall be considered to be the provider of the high-risk AI system, and shall be subject to i. a. the obligations under Article 16 AI Act if the high-risk system is placed on the market together with the product under the name or trademark of the product manufacturer or put into service under the name or trademark of the product manufacturer after the product has been placed on the market (Art. 25(3) AI Act). In such cases of extension, the plant owner integrating AI-driven robots might not only be considered as a deployer but also a 'provider'. This is of central significance as (differently from

‘deployers’) most obligations apply to ‘providers’ (Wendehorst, 2024a), who are bearing full responsibility for the AI systems’ compliance with the AI Act in substance and formalities – though in some cases it might be sufficient to refer to existing documentation so far kept by the former provider (Gössl, 2024).

Human-centred Industrial Robots as AI systems

The precondition of any risk assessment is the qualification of an industrial robot as an AI system, hence.

> “a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments” (Art. 3(1) AI Act).

Meanwhile, the European Commission (EC, 2025) has issued non-binding guidelines on the definition and its seven main elements as required by Art. 96(1) (f) AI Act. The element of inferencing how to generate output is seen as a key characteristic to set apart AI systems from “simpler traditional software systems or programming approaches, and should not cover systems that are based on the rules defined solely by natural persons to automatically execute operation” (Recital 12 AI Act). AI techniques enabling inference “include machine learning approaches” (Recital 12 AI Act), which includes supervised learning (learning from labelled data paired with the correct output; e.g. image classification); unsupervised learning (learning from patterns without predefined labels or outputs; e.g. anomaly detection), including self-supervised learning (learning without predefined labels, creating own labels and objectives; e.g. image recognition systems predicting missing pixels, language models predicting next tokens); reinforcement learning (learning by rewards/try and error; e.g., robot arm for grasping; autonomous mobile robots); deep learning (utilizing neuronal networks for representation learning) (EC, 2025). Other relevant techniques are “logic and knowledge-based approaches that infer from encoded knowledge or symbolic representation of the task to be solved” (Recital 12 AI Act) to “apply formal logic, predefined rules or ontologies to new situations” (EC, 2025, p. 7). The guidelines also label systems that may be seen as outside the scope of the AI system definition, such as systems for improving mathematical optimization, basic data processing, systems based on classical heuristics, and simple prediction systems (EC, 2025). Against this backdrop, typical scenarios and the relevant obligations for human-centred industrial robots can be exemplarily categorized according to the risk classification provided by the AI Act.

Prohibited Risks

Prohibited risks concern the placing on the market (Art. 3(9) AI Act), the putting into service (Art. 3(11) AI Act; sometimes limited to the specific purpose) and/or the use (cf. Art. 3(4) AI Act), of AI systems for certain types of manipulation, exploitation of group-related vulnerabilities, social scoring, risk assessments in the area of criminal prosecution, facial recognition databases, emotion inference, biometric categorisation or remote biometric identification (Art. 3(41), (35); Art. 5(1) AI Act). Having a closer look to the specifications of these, initial relevance for industrial human-robot settings can at most be attributed to emotion detection (Art. 5(1) (f) AI Act) prohibiting “AI systems to infer emotions of a natural person in the areas of workplace and education institutions, except where the use of the AI system is intended to be put in place or into the market for medical or safety reasons”. Emotion detection might be important for the robot to be able to assess and adapt to the human counterpart’s state, e.g., fatigue. As far – and only as far – as this is related to the safety of the worker or third persons (including the training of the robots), it might be justified subject to strict proportionality (Wendehorst, 2024b). Dual use of collected purposes, e.g., for performance assessments, is prohibited.

High Risks

High risk systems are AI systems which either are subject to a third-party conformity assessment (Art. 3(20) AI Act) under product safety law in accordance with Annex 1, either as a product itself or as a safety component (Art. 3(14) AI Act) of a product (Art. 6(1) AI Act) or are referred to in Annex III (Art. 6(2) AI Act), including its amendments (Art. 7 AI Act). Regarding product safety, Regulation 2006/42/EC on machinery and its successor Regulation (EU) 2023/1230 (applicable from 2027 on) are of special relevance for industrial human-robot systems. “Machinery that has embedded systems with fully or partially self-evolving behaviour using machine learning approaches ensuring safety functions that have not been placed independently on the market” (Art. 6, Annex I Part 1 No. 1 Regulation (EU) 2023/1230) are subject to a conformity assessment procedure according to Art. 25(2) Regulation (EU) 2023/1230, and therefore to be regarded as high-risk systems. Similar relevance is

to be attributed to AI systems in the area of biometrics related to remote identification (e.g. for adapting robot settings to individual attributes of workers), categorisation according to sensitive or protected attributes or characteristics (e.g. for detection of illnesses) or non-prohibited emotion detection (i.e. for medical or safety purposes (cf. Art. 5 (1) (f); Art. 6(2), Annex III No. 1 AI Act) as well as "AI systems intended to be used to make decisions affecting terms of work-related relationships, the promotion or termination of work-related 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" (e.g. to adapt robots to current the efficiency of the human co-worker) (Art. 6(2), Annex III No. 4(b) AI Act) (cf. Ruschemeier, 2024). In contexts of industrial human-robot collaboration, derogations foreseen in Art. 6(3)1 AI Act (narrow procedural task; improving the result of a previously completed human activity; detection of or deviations from prior decision-making patterns; preparatory tasks to an assessment) are generally not applicable, as a reverse exception is foreseen for AI systems performing profiling (Art. 6(3)2 AI Act), which is

> "any form of automated processing of personal data [Art. 3(50) AI Act] consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements", Art. 3(52) AI Act, Art. 4(4) Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR).

High-risk AI systems shall comply with the requirements (Art. 8 AI Act) related to risk management systems (Art. 9 AI Act); data and data governments (Art. 10 AI Act); technical documentation (Art. 11 and Annex IV AI Act); record keeping (Art. 12 AI Act); transparency and provision of information to deployers (Art. 13 AI Act); human oversight (Art. 14 AI Act); and accuracy, robustness and cybersecurity (Art. 15 AI Act). Its providers have a wide range of obligations, non-exclusively (Eisenberger, 2024) listed in Art. 16 AI Act, referring to e. g. compliance with the aforementioned requirements; indication of systems with name, trade name or trade mark, contact address; quality management system (Art. 17 AI Act); documentation (Art. 18 AI Act); logs (Art. 19 AI Act); conformity assessments (Art. 43, Annexes VI, VII AI Act); EU declaration of conformity (Art. 47, Annex V AI Act); CE marking (Art. 48 and 3(24) AI Act); registration (Art. 49(1) AI Act); corrective actions and information (Art. 20 AI Act); and conformity demonstration. Deployers' obligations concern measures to ensure usage in accordance with the instructions; assignment of human oversight; input data (Art. 3(33) AI Act); monitoring, information of provider, distributor and relevant market surveillance authorities as well as suspension; logs; information of workers' representatives and affected workers; data protection impact assessment; information of AI-based decision making or assistance; and cooperation with authorities (Art. 26 AI Act). By contrast, obligations to conduct a fundamental rights impact assessment (Art. 27 AI Act) are not relevant for industrial human-robot settings.

Transparency Risks

Some AI systems are seen as particularly sensitive due to their capability to create realistic, deceptively genuine synthetic content, and are therefore met with transparency obligations for providers and/or deployers (Art. 50 AI Act). The purpose is not to prohibit but to create awareness and avoid deception (Martini, 2024). Even if AI systems are classified as high-risk, the respective obligations apply in parallel to possible other obligations (Art. 50(6) AI Act). In the context of human-robot collaboration, it is the provider to generally ensures that AI systems intended to interact directly with workers through a robot are designed and developed in such a way that the natural persons concerned are informed that they are interacting with an AI system (Art. 50(1) AI Act). As far as AI systems used for emotion recognition are not prohibited (Art. 5(1) (f) AI Act), and disregarding whether they are not intended for this purpose and, therefore, qualifying as high-risk (Art. 6(2), Annex III No. 1(c) AI Act), they require the deployer to inform the exposed natural person (here: esp. the human co-worker) accordingly and comply to the GDPR (Art. 50(3) AI Act). This includes the general prohibition of processing special categories of personal data (Art. 9 GDPR), in our context, e.g., revealing racial or ethnic origin, trade union membership, genetic data, biometric data (Art. 3(34) AI Act) for uniquely identifying a natural person, or data concerning health.

General-Purpose Risks and Systemic Risks

Regularly, an AI model is seen as to have a general-purpose, if it "displays significant generality and is capable of competently performing a wide range of distinct tasks […] that can be integrated into a variety of downstream systems or applications"; included are AI models "trained with a large amount of data using self-

supervision at scale" (Art. 3(63) AI Act). The provider of any such model has particular obligations in light of the potential risks.

> "As the models they provide may form the basis for a range of downstream systems, often provided by downstream providers [Art. 3(68) AI Act] that necessitate a good understanding of the models and their capabilities, both to enable the integration of such models into their products, and to fulfil their obligations under this or other regulations" (Recital 101).

These obligations relate to the technical documentation of the model; information and documentation for providers of AI systems intending to integrate the model; a compliance policy; and a template summary related to the training data (Art. 53(1) AI Act, Annex XI, XII). A derogation may apply to free and open-source licensed AI models (Art. 53(2) AI Act).

A so-called general-purpose AI model might further qualify as a systematic risk, i.e.

> "a risk that is specific to the high-impact capabilities [Art. 3(64) AI Act] of general-purpose AI models, having a significant impact on the Union market due to their reach, or due to actual or reasonably foreseeable negative effects on public health, safety, public security, fundamental rights, or the society as a whole, that can be propagated at scale across the value chain" (Art. 3(65) AI Act).

To be classified as a systemic risk, in the first alternative, it has to have "high impact capabilities evaluated based on appropriate technical tools and methodologies, including indicators and benchmarks" (Art. 51(1) (a) AI Act). This is presumed when "when the cumulative amount of computation used for its training measured in floating point operations [FLOPs] is greater than 10^{25}" (Art. 51(2) AI Act; see Art. 3(67) AI Act for a definition of FLOPs). End of 2023, this scale was only topped by Gemini and GPT-4 (Sastry et al., 2024). In the second alternative, "based on a decision of the Commission […] it has capabilities or an impact equivalent […] having regard to the criteria set out in Annex XIII" (Art. 51(3) AI Act). Despite their specific industrial purpose, considering the growing demand for industrial agility and communication with human co-workers, as well as the rapid AI development, integrating such general-purpose AI with systemic risks into human-centred robots is a realistic scenario, especially when it is linked to the AI used in the administrative and managerial departments of the same plant. The constitutive (Bernsteiner, Schmitt, 2024) decision on the classification as a systemic risk is with the European Commission (Art. 52 AI Act). Once classified as such, the provider has additional obligations to perform model evaluation; to assess and mitigate possible systemic risks at Union level; to keep track, document, and report; as well as to ensure cybersecurity (Art. 55(1) AI Act). Relying on codes of practice (Art. 56 AI Act) may suffice to prove compliance (Art. 55(2) AI Act).

Minimal Risks

Risks not qualifying for one of the above classifications are seen as minimal. Examples could be voice-controlled robots without integration of general-purpose AI performing industrial tasks and responding to commands not designed for critical decision-making. In such cases, the only specific obligation posed on the plant owner is to "take measures to ensure, to their best extent, a sufficient level of AI literacy (Art. 3(56) AI Act) of their staff and other persons dealing with the operation and use of AI systems on their behalf, taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used" (Art. 4 AI Act). This obligation is the same for all risk classifications. Apart from that, plant owners with minimal risk AI systems are invited to apply the developed Codes of Conduct (Art. 95 AI Act) voluntarily (Ebers, 2024), including the EU's Ethics Guidelines for Trustworthy AI (High-Level Expert Group, 2019).

Conclusions

This legal assessment has proven the high relevance of the AI Act for industrial human-robot settings. As AI evolves exponentially, so does its significance for industrial and national agility and resilience. Obligations vary widely according to risk classification and the obligated operator. Coordination and information flows between providers and deployers of related AI systems are key. In many instances, the plant owner will become a provider himself or herself, thus extending obligations drastically. Design and implementation of human-centred robotic scenarios, thus, should be well planned, structured, documented, and constantly evaluated. The respective AI models and AI systems need to be legally compliant and human-centred by design. The extent to which a commitment to external and abstract norms (such as laws or the principle of non-harmfulness towards humans) can be inscribed in a learning system remains an open question. To provide an answer, an

unprecedented dialogue across disciplinary fields is needed. Limitations of the study are seen in the restricted framework of this contribution and the novelty of the involved legal aspects that will have to be explored and further developed by legislation, jurisdiction, and legal commentators throughout the next years. The focus of the contribution was only on standards and implications related to the AI Act. Other relevant legal areas, such as Product Liability Law, Product Safety Law, Machinery Law, Technical Standards, Data Protection Law, Copyright and IP Law, or Labour Law, and their respective interplay with the AI Act need similar attention.

Acknowledgements

The author would like to thank Dorit Borrmann, Kai Diethelm, Bastian Engelmann, Magda Gregorová, Tanja Henking, Tobias Kaupp, Alma Kolleck, Pascal Meißner, and Volker Willert (all professors at the Technical University of Applied Sciences Würzburg-Schweinfurt) for their expertise and valuable input.

References

1. Bear, D. M., Fan, C., Mrowca, D., Li, Y., Alter, S., Nayebi, A., Schwartz, J., Fei-Fei, L., Wu, J., Tenenbaum, J. B., & Yamins, D. L. K. (2020). Learning physical graph representations from visual scenes. In *34th Conference on Neural Information Processing Systems (NeurIPS)*, 1–23. https://doi.org/10.48550/arXiv.2006.12373
2. Bernsteiner, C., & Schmitt, T. R. (2024). Art. 52 AI Act. In M. Martini, & C. Wendehorst (Eds.), *KI-VO: Verordnung über künstliche Intelligenz*, 799–807. Beck.
3. Boget, Y., Gregorova, M., & Kalousis, A. (2024). Discrete graph auto-encoder. *Transactions on Machine Learning Research*, 3, 1–26. https://openreview.net/pdf?id=bZ80b0wb9d
4. Breque, M., De Nul, L., & Petridis, A. (2021). *Industry 5.0: Towards a sustainable, human-centric and resilient European industry*. European Commission Policy Brief. https://op.europa.eu/en/publication-detail/-/publication/468a892a-5097-11eb-b59f-01aa75ed71a1/
5. Brunke, L., Greeff, M., Hall, A. W., Yuan, Z., Zhou, S., Panerati, J., & Schoellig, A. P. (2022). Safe learning in robotics: From learning-based control to safe reinforcement learning. *Annual Review of Control, Robotics, and Autonomous Systems*, 5, 411–444. https://doi.org/10.1146/annurev-control-042920-020211
6. Donath, J. (2020). Ethical issues in our relationship with artificial entities. In M. D. Dubber, F. Pasquale, & S. Das (Eds.), *The Oxford Handbook of Ethics of AI*, 52–73. Oxford Academic. https://doi.org/10.1093/oxfordhb/9780190067397.013.3
7. Ebers, M. (2024). Regulierung generativer künstlicher Intelligenz in der KI-VO. In M. Ebers, & B. M. Quarch (Eds.), *Rechtshandbuch ChatGPT: KI-basierte Sprachmodelle in der Praxis*, 43–91. Nomos.
8. EC. (2024, August 1). *Artificial Intelligence – Questions and Answers.* https://ec.europa.eu/commission/presscorner/detail/en/qanda_21_1683
9. EC. (2025). *Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act).* C (2025) 924 final. 6/2/2025. https://ec.europa.eu/newsroom/dae/redirection/document/112455
10. Eisenberger, I. (2024). Art. 16 AI Act. In M. Martini, & C. Wendehorst (Eds.), *KI-VO: Verordnung über künstliche Intelligenz*, 467–474. Beck.
11. Gössl, S. L. (2024). Art. 25 AI Act. In M. Martini, & C. Wendehorst (Eds.), *KI-VO: Verordnung über künstliche Intelligenz*, 538–557. Beck.
12. High-Level Expert Group on Artificial Intelligence (HLEG). (2019). *Ethics guidelines for trustworthy AI*. https://op.europa.eu/en/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1
13. Kroemer, O., Niekum, S., & Konidaris, G. (2022). A review of robot learning for manipulation: Challenges, representations, and algorithms. *Journal of Machine Learning Research*, 22(1), 1395–1476. https://www.jmlr.org/papers/volume22/19-804/19-804.pdf
14. Lin, C. J., & Lukodono, R. P. (2025). Learning performance and physiological feedback-based evaluation for human–robot collaboration. *Applied Ergonomics*, *124*, 104425. https://doi.org/10.1016/j.apergo.2024.104425
15. Martini, M. (2024). Art. 50 AI Act. In M. Martini, & C. Wendehorst (Eds.), *KI-VO: Verordnung über künstliche Intelligenz*, 760–788. Beck.
16. Pasquale, V. D., Farina, P., Fera, M., Gerbino, S., Miranda, S., & Rinaldi, M. (2024). Human robot-interaction: a conceptual framework for task performance analysis. *IFAC PapersOnline*, 58(19), 79–84. https://doi.org/10.1016/j.ifacol.2024.09.096
17. Ramapuram, J., Gregorova, M., & Kalousis, A. (2020). Lifelong generative modelling. *Neurocomputing*, 404, 381–400. https://doi.org/10.1016/j.neucom.2020.02.115
18. Ruschemeier, H. (2024). Annex III AI Act. In M. Martini, & C. Wendehorst (Eds.), *KI-VO: Verordnung über künstliche Intelligenz*, 1133–1157. Beck.
19. Sanfilippo, F., Zafar, M. H., & Zambetta, F. (2025). From caged robots to high-fives in robotics: Exploring the paradigm shift from human-robot interaction to human-robot teaming in human-machine interfaces. *Journal of Manufacturing Systems*, 78, 1–25. https://doi.org/10.1016/j.jmsy.2024.10.015

20. Sastry, G., Heim, L., Belfield, H., Andljung, M., Brundage, M. Hazell, J., O'Keefe, C., Hadfield, G. K., Ngo, R., Pilz, K., Gor, G., Bluemke, E., Shoher, S., Egan, J., Trager, R. F., Avin, S., Weller, A., Bengio, Y., & Coyle, D. (2025). *Computing power and the governance of artificial intelligence*. 1–103. https://doi.org/10.48550/arXiv.2402.08797
21. Schmager, S., Pappas, I. O., & Vassilakopoulou, P. (2025). Understanding human-centred AI: A review of its defining elements and a research agenda. *Behaviour & Information Technology,* 1–40. https://doi.org/10.1080/0144929X.2024.2448719
22. Wendehorst, C. (2024a). Art. 3 AI Act. In M. Martini, & C. Wendehorst (Eds.), *KI-VO: Verordnung über künstliche Intelligenz*, 140–234. Beck.
23. Wendehorst, C. (2024b). Art. 5 AI Act. In M. Martini, & C. Wendehorst (Eds.), *KI-VO: Verordnung über künstliche Intelligenz*, 240–286. Beck.
24. Wulfmeier, M., Byravan, A., Hertweck, T., Higgins, I., Gupta, A., Kulkarni, T., Reynolds, M., Teplyashin, D., Hafner, R., Lampe, T., & Riedmiller, M. (2021*).* Representation matters: Improving perception and exploration for robotics*.* In *IEEE International Conference on Robotics and Automation (ICRA)*, Xian, China. https://doi.org/10.48550/arXiv.2011.01758

Į ŽMOGŲ ORIENTUOTA ROBOTIKA IR ES DI AKTAS: ATRINKTI STANDARTAI IR PASEKMĖS

Santrauka

Robotika ir dirbtinis intelektas yra svarbūs veiksniai, lemiantys verslo ir nacionalinį atsparumą, siekiant išlaikyti gamybą aukšto darbo užmokesčio šalyse, susiduriančiose su demografiniais iššūkiais. Abu šie veiksniai yra svarbūs siekiant, kad gamyba taptų lankstesnė ir greitesnė. Robotai ir žmonės turės glaudžiai bendradarbiauti. Būtinas pažangių autonominių sistemų kūrimas. Pagal ES pramonės 5.0 viziją, kuria siekiama sukurti tvarią, į žmogų orientuotą ir atsparią Europos pramonę, žmonės ir robotai turės dirbti taip glaudžiai, kad robotų programinė įranga turės būti kuriama nuo pat pradžių atsižvelgiant į žmogaus poreikius. Todėl taip pat turi būti atsižvelgiama į etines, teisines ir socialines pasekmes (ELSI). Teisinės pasekmės yra įvairiapusės – jos apima DI teisę, produkto atsakomybės teisę, produkto saugos teisę, mašinų teisę, techninius standartus, duomenų apsaugos teisę, autorių ir intelektinės nuosavybės teisę, darbo teisę ir kt. Šiame straipsnyje bus trumpai pristatytos reikiamos techninės savybės ir, remiantis jomis, nagrinėjamos atrinktos teisinės pasekmės bei su jomis susiję naujojo ES DI akto standartai. Šis įstatymas, kurio tikslas – užtikrinti teisingą žmogaus suvokimą, įsigaliojo 2024 m. rugpjūčio 1 d. ir bus taikomas etapais iki 2027 m. rugpjūčio 2 d. Ypatingas dėmesys bus skiriamas žmogaus interesams, gamintojo priskyrimui prie įpareigotųjų šalių (tiekėjo, produkto gamintojo, diegėjo, įgaliotojo atstovo ar platintojo) kategorijos, taip pat klasifikavimui pagal DI rizikos schemą (draudžiamos rizikos, didelės rizikos, skaidrumo rizikos, bendrosios paskirties rizikos ir sisteminės rizikos, taip pat minimalios rizikos) ir susijusioms prievolėms. Didelis dėmesys bus skiriamas pramoniniams žmogaus ir roboto sąveikos atvejams DI įstatyme. DI sparčiai vystantis, didėja ir jo svarba pramonės ir nacionaliniam lankstumui bei atsparumui. Įsipareigojimai labai skiriasi priklausomai nuo rizikos klasifikacijos ir įpareigotojo operatoriaus. Labai svarbus koordinavimas ir informacijos srautai tarp susijusių DI sistemų teikėjų ir diegėjų. Kadangi gamintojai patys gali tapti teikėjais, pareigos gali būti įvairesnės, nei iš pradžių manyta. Todėl žmogaus poreikiais grindžiamų robotų scenarijų kūrimas ir įgyvendinimas turėtų būti gerai suplanuotas, struktūrizuotas, dokumentuojamas ir nuolat vertinamas. Atitinkami DI modeliai ir DI sistemos turi atitikti teisės aktų reikalavimus ir būti sukurti žmogaus poreikiams tenkinti. Būtinas precedento neturintis dialogas tarp įvairių sričių specialistų.

Reikšminiai žodžiai: AI aktas, robotika, pramonė, didelės rizikos AI sistemos, bendrosios paskirties AI modeliai

Information about the author

dr. Ralf Roßkopf. Technical University of Applied Sciences Würzburg-Schweinfurt, Faculty of Applied Social Sciences, Center for Artificial Intelligence, Institute of Applied Social Sciences, Professor. Research fields: Artificial Intelligence Law, Public Law, Migration Law, Human Rights.
Email address: ralf.rosskopf@thws.de
ORCID: https://orcid.org/0000-0001-7364-8383