European Journal of Risk Regulation (2025), 1–21
doi:10.1017/err.2025.10058

ARTICLE

The EU AI Act and the Food System: How the European Union Ai Act Applies to Agrifood

Idse Lucien Val

Law, Wageningen Universiteit en Research, Wageningen, Netherlands
Email: idse.val@wur.nl

Abstract

Artificial Intelligence (AI) is increasingly being used in the agrifood sector to improve efficiency, safety and sustainability. The application of the European Union Artificial Intelligence Act's (AI Act) to the broad spectrum of agrifood AI systems has not been thoroughly analyzed. Therefore, this research article explores the AI Act's application to the agrifood sector by providing an overview of AI systems in the sector and applying the AI Act's risk-categorisation system to them. Section II provides an outline of the AI Act and its risk categorisation system. Section III gives an overview of agrifood AI systems and explains how the AI Act applies to them. The AI Act is most significantly applicable to AI safety components that are used in agricultural or agroforestry vehicles and other machinery. Although not many, there are also some types of agrifood AI systems that will be prohibited and that will have special transparency requirements under the AI Act. The paper also identifies potential sector-specific challenges such as a risk to food security, an open question regarding the extensiveness of the meaning of 'AI safety component' and the inattention of the AI Act to non-human centred values such as the environment, biodiversity and animal welfare.

Keywords: agrifood; AI Act; food system

I. Introduction

As time passes, artificial intelligence (AI) continues to permeate society and, accordingly, it has also found its way well into the agrifood value-chain.[1] Against a backdrop of growing global food demand, AI offers the theoretical promise of increasing food security and yields through more effective management of crops, more accurate prediction of crop yields, better animal health management and helping breed more reliable crop and livestock varieties.[2] In this vein, the European Union's Farm to Fork Strategy, a policy promoting sustainability across the EU food system, highlighted AI as one of the technologies that enables the transition towards a climate-neutral food system.[3] However, AI systems do not necessarily imply greater sustainability. For example, there are concerns that AI in agrifood can enable practices that conflict with environmental values, such as increased

[1] I Kutyauripo, M Rushambwa, and L Chiwazi, "Artificial Intelligence Applications in the Agrifood Sectors" 11 (2023) Journal of Agriculture and Food Research 100502 https://doi.org/10.1016/j.jafr.2023.100502.

[2] R Chamara and others, "Role of Artificial Intelligence in Achieving Global Food Security: A Promising Technology for Future" 6(2) (2020) Sri Lanka Journal of Food and Agriculture 43. http://doi.org/10.4038/sljfa.v6i2.88.

[3] European Commission, "A Farm to Fork Strategy for a Fair, Healthy and Environmentally-Friendly Food System" (Communication) COM (2020) 381 final, paragraph 3.1.

pesticide use as a result of a decrease in the cost of application, or as a result of farmers no longer having to be exposed to the chemicals during the application process.[4] Yet, while new technologies come with great promise, they also come with an inherent level of uncertainty and thus a risk potential. The existence of potential risks to important EU values like safety and human rights has prompted EU regulators to create a regulation on AI called the Artificial Intelligence Act (AI Act).[5] With the AI Act, the EU seeks to appropriately manage the risks to health, safety and fundamental rights that come with broad societal adoption of AI.[6]

This article explores how the AI Act's risk-categorisation system could apply to AI in the agrifood sector. The agrifood sector is treated as an integral whole in which AI will be used and in which it can affect core agrifood values such as food security, food safety, food traceability and others. The "agrifood sector" and "food system" are sometimes used synonymously.[7] Section II begins with a high-level overview of the AI Act, including the Regulation's basic components: the definition of AI, the risk-categorisation system and the requirements applicable to high-risk AI systems. Section III provides an overview of the types of AI currently used in the agrifood sector. This is followed by a non-exhaustive overview of agrifood AI systems that fit one of the AI Act's risk-categories. Finally, Section IV raises some unaddressed challenges of AI in the agrifood sector. By connecting the AI Act to the agrifood sector, this article seeks to contribute a sectoral perspective on the AI Act while offering insights for the betterment of the EU's risk governance of AI.

2. Europe's point of convergence on AI Law: the AI Act

1. Overview

The AI Act is an EU regulation, which means its rules will apply directly in all EU Member State jurisdictions. The legal basis of the AI Act lies in Article 114 and Article 16 of the Treaty on the Functioning of the European Union (TFEU). This means that the Act has both the proper functioning of the internal market and the fundamental right to protection of personal data respectively as a justificatory rationale. The purpose statement mentions the functioning of the internal market, promoting the uptake of human centric AI and ensuring a high level of protection to health, safety and fundamental rights as enshrined in the EU Charter.[8]

[4] M Ryan, "The Social and Ethical Impacts of Artificial Intelligence in Agriculture: Mapping the Agricultural AI Literature" 38 (2023) AI & Society 2473. <https://link.springer.com/article/10.1007/s00146-022-01373-2>

[5] 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 (2023) 206 final. (Hereafter: AI Act).

[6] Article 1 AI Act.

[7] While agriculture enjoys a special legal status in the EU, the technical focus of this article justifies a scope on applications in the agrifood sector as a domain in an encompassing fashion. This also fits the broad definition of the General Food Law Regulation (Regulation (EC) 178/2002 of the European Parliament and of the Council of 28 January 2002 laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety [2002] OJ L31/1), where food covers any stage of production, processing and distribution of food, and is in line with the spirit of the new Vision on Agriculture and Food that speaks of the agri-food system (European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Vision for Agriculture and Food – Shaping together an attractive farming and agri-food sector for future generations COM(2025) 75 final, 19 February 2025).

[8] Article 1(1) AI Act.

The AI Act is part of the broader European AI strategy,[9] which also included the adoption of the now withdrawn draft proposal for a AI liability Directive.[10] Other regulatory initiatives that contain rules that touch on AI are: the Digital Services Act,[11] the Digital Markets Act,[12] the Machinery Regulation,[13] the Data Governance Act[14] and the Product Liability Directive.[15]

The adoption of the AI Act was a complex process marked by extensive debate and revision since the European Commission's initial White Paper in February 2020. The Act's first draft proposal,[16] published in April 2021, faced numerous critiques, including concerns over its definitions,[17] coverage of risks,[18] and regulatory approach.[19] During the legislative process many parts of the AI Act were adapted to respond to critiques and political requests. Some notable amendments during the legislative process were the use of the OECD definition of AI and the inclusion of general purpose AI (GPAI) models as a special risk category. Finally, after extensive negotiations and amendments, the EU's legislative bodies reached a political agreement on the final text of the AI Act on December 9, 2023, with the Act having come into force August 1, 2024.

The AI Act falls within the domain of risk regulation. Risk-based regulation is a regulatory approach which entails that a regulator introduces levels of control proportional to ascertained risks by taking into consideration both specific harms and

[9] European Commission, "European Approach to Artificial Intelligence" (European Commission, 28 October 2024) <https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence>, accessed 28 November 2024.

[10] European Commission, Proposal for a Directive of the European Parliament and of the Council on Adapting Non-Contractual Civil Liability Rules to Artificial Intelligence (AI Liability Directive), COM(2022) 496 final (withdrawn). (hereafter: Draft AI Liability Directive (withdrawn).

[11] European Parliament and Council Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L277/1.

[12] European Parliament and Council Regulation (EU) 2022/1925 of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2022] OJ L265/1.

[13] European Parliament and Council Regulation (EU) 2023/1230 of 14 June 2023 on machinery and repealing Directive 2006/42/EC of the European Parliament and of the Council and Council Directive 73/361/EEC (Text with EEA relevance) [2023] OJ L165/1. (hereafter: Machinery Regulation).

[14] European Parliament and Council Regulation (EU) 2022/868 of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance) [2022] OJ L152/1.

[15] Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC [2024] OJ L 2024/2853, 18.

[16] "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 – General approach" (Interinstitutional File: 2021/0106(COD), Permanent Representatives Committee (Part 1) to Council, No prev. doc.: 14336/22, No. Cion doc.: 8115/21), Amendments; AI Mandates (20 June 2023) <https://artificialintelligenceact.eu/wp-content/uploads/2023/08/AI-Mandates-20-June-2023.pdf>, accessed 30 April 2025.

[17] B Casey and MA Lemley, "You Might Be a Robot" (2019) 105 Cornell Law Review 287.

[18] J Chamberlain, "The Risk-Based Approach of the European Union's Proposed Artificial Intelligence Regulation: Some Comments from a Tort Law Perspective" (2023) 14 European Journal of Risk Regulation (EJRR); J De Cooman, "Humpty Dumpty and High-Risk AI Systems: The Ratione Materiae Dimension of the Proposal for an EU Artificial Intelligence Act" (2022) 6 Market and Competition Law Review 49; K Grieman and J Early, "A Risk-Based Approach to AI Regulation: System Categorisation and Explainable AI Practices" (2023) 20 SCRIPTed: A Journal of Law, Technology and Society 56; J Laux, S Wachter and B Mittelstadt, "Trustworthy artificial intelligence and the European Union AI act: On the conflation of trustworthiness and acceptability of risk" Regulation & Governance.

[19] N Smuha et al, "How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act" (5 August 2021) University of Birmingham LEADS Lab, <https://ssrn.com/abstract=3899991> accessed 8 May 2025.

the likelihood of them occurring.[20] Justificatory to a risk-based approach is a degree of uncertainty.[21] The purpose of a risk-based approach is about managing, preventing or mitigating potential harms by anticipating them in a probabilistic manner and a risk-based regulation can thus be conceived as treading the limits of what a regulation can realistically be expected to achieve in uncharted legal waters.[22]

The risk-based approach of the AI Act resulted in a tiered regulatory structure of AI systems, with several risk categories that each represent a tier of associated risk and a respective and proportional strictness of applicable rules. The risk-categories of the AI Act are: prohibited AI practices presenting unacceptable risks (Article 5), high-risk AI practices which have mandatory requirements (Article 6), AI practices that must provide transparency about their use (Article 50), general-purpose AI models (Article 51 & 52) and AI practices that do not fit any of the former risk-categories to which voluntary codes of conduct could be drawn up (Article 95).

The AI Act is also in a sense a product safety regulation.[23] The requirements for providers of high-risk AI covered in Section 2 and 3 of the AI Act all have product safety and accountability of the provider of the AI product in mind.

The withdrawn draft AI Liability Directive sought to level the playing field for victims of AI-related harm by tackling information asymmetry. It would have empowered courts to compel disclosure of evidence about high-risk AI systems and introduced a rebuttable presumption of causality in fault-based claims. The AI Liability Directive was therefore intended to prescribe additional rules affecting AI systems labelled high-risk under the AI Act, whereas now, such systems have no special liability rules applicable to them.

Now, with the AI Liability Directive withdrawn, liability of AI is only regulated on an EU level through the full harmonisation Product Liability Directive, where AI is shared under "software" which is considered a "product."[24] This Directive entails that when natural persons suffer damage as a result of a defective AI system, they are entitled to compensation under a Member State strict product liability scheme.

In terms of scope, the AI Act applies to providers of AI systems in the European Union, irrespective of whether they are located in the EU or in a third country.[25] This means if an AI system is sold in an EU Member State, the provider of that system must comply with the AI Act. The Act will also apply to users of AI that are located or have their establishment within the EU.[26] Anyone in the EU that uses AI is in principle covered by the AI Act. Lastly, the Act applies to providers or deployers of AI systems located in third countries where the output of that system is used in the EU.[27] With this, the AI Act has extraterritorial effect, meaning the EU effectively exports its regulatory standards globally, leveraging its market power to influence compliance with its rules beyond its borders, also sometimes referred to as "the Brussels Effect."[28] An example of this effect is an AI chatbot that is developed and provided by a Chinese company, that is deployed by a US social media company and that then interacts with EU citizens. Here, the Chinese provider would be bound by the AI Act, since the output of the AI System is used in the EU. It has been argued that the

[20] H Rothstein and others, "The risks of risk-based regulation: Insights from the environmental policy domain" 32 (2006) Environment International 1056, p 1057.

[21] MBA Van Asselt, E Vos and B Rooijackers, 'Science, Knowledge and Uncertainty in EU Risk Regulation' (2009) Uncertain Risks Regulated 359, p 360.

[22] Rothstein (n 20), p 1057.

[23] M Veale and F Zuiderveen Borgesius, "Demystifying the Draft EU Artificial Intelligence Act" 22(4) (2021) Computer Law Review International 97, available at https://doi.org/10.48550/arXiv.2107.03721

[24] Art 4(1) & Recital 13 Directive (EU) 2024/2853.

[25] Art 2(1a) AI Act.

[26] Art 2(1b) AI Act.

[27] Art 2(1c) AI Act.

[28] A Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press 2020).

extraterritorial approach closely mirrors that of the General Data Protection Regulation (GDPR),[29] which has been argued to lack in its effective enforcement for its global reach to be more than theoretical.

2. What is in the AI Act?

a. Definition of AI

The material scope of the AI Act is delineated by the definition of AI. An "*Artificial intelligence system*" is defined as "*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.*"[30]

Recital 6 of the AI Act clarifies how these terms should be interpreted and this interpretation aligns closely with the OECD definition, on which the definition was based.[31] The part "*infers from the input it receives, how to generate outputs*" is the key element of the definition; it signals the flow of information entering a system, the system running some statistical, logical or mathematical operations on the information and an output that is generated by the system based on those operations.[32] These outputs so generated may come in various forms, which is clarified by specifying that the definition covers outputs "*such as predictions, content recommendations, or decisions*." The AI Act recognises that AI systems act with varying levels of autonomy and possibly adaptiveness, which is further explained in Recital 6 as: '*some degree of independence of actions from human involvement and capabilities to operate without human intervention. The adaptiveness of an AI system refers to its self-learning capabilities, which allow it to change and adapt while in use*'.

With this definition and specifically the notion of inference, the regulator distinguishes AI from regular non-AI software.[33] What constitutes "Artificial Intelligence" under the AI Act covers a spectrum, from arguably less "intelligent" to more "intelligent" AI. The majority of systems will be simple to classify under this definition, but where the line between regular software and AI will lie exactly might not always be clear, as Hacker has also pointed out,[34] and will likely be developed through experience and caselaw.

b. Prohibited AI practices

The first risk-category of the AI Act consists of systems that are considered to introduce unacceptable risks to human rights or safety and are therefore prohibited. Article 5 of the AI Act lists types of AI application that are prohibited. The list contains prohibitions on using AI to create defects of will by manipulating or targeting individuals or groups of vulnerable people (1a & 1b). Beyond this the list contains prohibitions on AI systems used for surveillance: social scoring (1c), predictive policing (1d), expanding facial recognition

[29] 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.

[30] Art 3(1) AI Act.

[31] S Russell, K Perset, and M Grobelnik, "Updates to the OECD's Definition of an AI System Explained" (29 November 2023) <https://oecd.ai/en/wonk/ai-system-definition-update>, accessed 12 February 2024.

[32] Ibid.

[33] The relationship between AI and regular software can be seen as a genus-species relationship. An example of which is found in the under the Product Liability Directive (EU) 2024/2853 where AI is considered "software," while certainly not all software is AI.

[34] P Hacker, "Comments on the Final Trilogue Version of the AI Act" (23 January 2024) <https://ssrn.com/abstract=4757603>, accessed 2 October 2024.

databases (1e), inferring emotion in the workplace or education (1f), biometric categorisation (1g), and "real-time" remote biometric identification in public spaces (1h). The "prohibitions" on AI systems used for social scoring and "real-time" remote biometric identification used in law enforcement are somewhat misleading, since there are conditions under which such systems are exempted.[35] At first glance, the list of prohibited AI does not seem to have strong implications for the agrifood sector, although some agrifood AI systems might fall within its scope (see Section III).

c. High-risk AI practices

i. Qualification as high-risk. The second risk-category of the AI act consists of systems that are deemed to pose a *high risk* to human rights or safety. Mandatory requirements are applicable to AI systems that are considered to pose a high risk.[36] What systems qualify as high-risk are found in Article 6 of the AI Act. There are two basic grounds for a system to be qualified as such.

The first ground is found in paragraph 1 of Article 6 and refers to when an AI system is in some way used as a safety component of a product, or when the AI system itself is a product that is regulated by one of the listed EU harmonisation legislations and is, based on that regulation, required to undergo a third-party conformity assessment.[37] A safety component is "*a component of a product or of an AI system which fulfils a safety function for that product, or the failure or malfunctioning of which endangers the health and safety of persons or property*."[38] The list of relevant EU harmonisation legislations is found in Annex I of the AI Act and contains Regulations and Directives on safety for various things like toys, civil aviation security or medical devices.[39] The most notable Regulations in the list for the agrifood context are Regulation (EU) No 167/2013 on the approval and market surveillance of agricultural and forestry vehicles and the Machinery Regulation, which together cover a large range of agricultural equipment and machinery.

The second ground for an AI system to be categorized as high-risk is found in Article 6(2) and refers to when a system is used in a field of application that is considered sensitive because of its nature such as law enforcement and migration. Annex III lists such areas of application.[40] Noteworthy for the agrifood context is the high risk classification of AI systems managing "*critical infrastructure*" in Annex III (2). Annex III (2) mentions "*Critical infrastructure: AI systems intended to be used as safety components in the management and operation of critical digital infrastructure, road traffic, or in the supply of water, gas, heating or electricity*." More explanation on the applicability of this to the agrifood sector follows in Sections 3 and 4. Exempted from the high-risk classification based on Article 6(2) are systems that do not pose a significant risk of harm to the health, safety or fundamental rights of natural persons, for example by not materially influencing the outcome of decision-making Article (6(3)).

ii. Requirements for high-risk AI systems. The qualification of an AI system as high-risk requires compliance with Chapter 2 of the AI Act. High-risk AI systems must have a risk management system (Article 9), use adequate, representative, and well-managed data

35 Art 5(1c) & 5(1h) AI Act.
36 Chapter 2 and 3 of Title III of the AI Act.
37 Art 6(1) AI Act.
38 Art 3(14) AI Act.
39 Annex I of the AI Act contains the complete list of harmonization regulations.
40 The high-risk AI system areas listed in Annex III of the AI Act include: biometric identification and categorisation of natural persons; management and operation of critical infrastructure; education and vocational training; employment, workers management and access to self-employment; access to essential private and public services; law enforcement; migration, asylum and border control management; and administration of justice and democratic processes.

(Article 10), include technical documentation (Article 11), maintain records (Article 12), ensure transparency for deployers or users (Article 13), enable human oversight (Article 14), and be accurate, robust, and secure (Article 15).

Providers are responsible for ensuring compliance (Article 16), implement a quality management system (Article 17), keep documentation and logs (Articles 18 & 19), conduct conformity assessments (Article 43), issue EU declarations of conformity (Article 47), affix CE markings (Article 48), and meet registration obligations (Article 49). Providers must also address non-compliance or malfunctions (Article 20), demonstrate conformity when requested (Article 21), and meet accessibility requirements per EU Directives 2016/2102 and 2019/882. Complying with these rules is estimated to be a costly continuous practice. The AI Act includes additional rules for importers, distributors and users of high-risk AI systems, but these are not covered here

d. AI systems with transparency obligations

The third risk-category consists of AI systems that interact directly with natural persons (Article 50) and that therefore have a special transparency requirement. Users must be informed about direct interactions with AI systems in general, AI-generated content must be labelled, people must be informed when AI emotion recognition or biometric categorisation is used on them and deepfakes must be labelled except in cases of obvious, artistic, satirical or fictional contexts. The special transparency obligation does not apply to AI systems authorised by law to detect, prevent, investigate, or prosecute criminal offenses.

e. General-purpose AI

*i. Definition of general-purpose AI***.** The fourth and last risk-category of the AI Act are general-purpose AI (GPAI) systems, which is found in is in Article 3(63) and Chapter V of the AI Act. GPAI was introduced relatively late in the legislative process to keep up with rapid innovations of the past years. The term "general-purpose AI" is intended to capture highly capable systems like chat-GPT, because they were thought to possess an inherent risks related to unforeseeable use cases. The main characteristic that sets GPAI apart from regular AI is that it must contain "*significant generality*" and must be "*capable to competently perform a wide range of distinct tasks*."[41] The Recitals mention that the "*generality*" of a model can be determined by the model size and that models with at least a billion parameters that used self-supervision at scale are considered to have it.[42] Typical examples of such models are generative models like GPT-4 and Llama-2.[43]

*ii. General-purpose AI with systemic risks***.** According to Article 51 of the AI Act, a GPAI model is classified as posing a "*systemic risk*" when "*it has high impact capabilities*," or, when the Commission decides that a model has capabilities or an impact equivalent to the former. "*High impact capabilities*" are assumed present when the cumulative amount of computation used for the model exceeds a compute threshold of 10^{25} floating point operations or FLOPs.[44] A heuristic like this is questionable because the amount of computation used in training is not necessarily correlated with model performance and a

[41] Art 3(63) AI Act.

[42] Recital 98 AI Act.

[43] Recital 99 AI Act; OpenAI, "GPT-4 Technical Report" (2023), available at <https://openai.com/research/gpt-4>, accessed 28 November 2024; H Touvron and others, "Llama 2: Open Foundation and Fine-Tuned Chat Models" (arXiv, 19 July 2023) <https://doi.org/10.48550/arXiv.2307.09288>.

[44] Recital 60(n) AI Act.

FLOP threshold will likely deprecate over time.[45] However, the Commission can amend this threshold, as well as other benchmarks or indicators when AI inevitably evolves further.[46]

f. Other parts of the AI Act

Outside the risk-categorisation system, the AI Act contains several other provisions relating to things such as measures in support of innovation,[47] rules on governance,[48] post-market monitoring, reporting duties and surveillance,[49] and penalties.[50]

Having outlined the AI Act, the next section provides an overview of AI in the agrifood sector and several examples of agrifood AI systems matching the risk-categories of the AI Act.

3. The AI Act and the agrifood sector

1. AI technologies in agrifood

AI is an umbrella term that describes the field of computer science that tries to have computers conduct tasks that typically require human intelligence.[51] These tasks include reasoning, learning, perceiving and decision-making and contains several subfields, such as machine learning, natural language processing, robotics, and knowledge representation.[52] Uses of AI in the agrifood sector span multiple functional domains, including sensing and data gathering, predictive modelling, planning and decision-support and natural perception, analytics and robotics, all of which present challenges and opportunities, which can contribute to enhancing productivity and sustainability if addressed properly.[53]

The large increase of agrifood AI is the result of the broader digitalisation of the industry with increasing adoption of digital technologies such as Internet(s) of Things (IoT) and big data processing. An Internet of Things, or IoT, refers to a digital network, or "internet," of sensors, devices and machines that can collect and share information between each other.[54] These "things" can help collect vast amounts of data, which can be used to inform decision-making and to develop AI technologies.[55] Digitalisation of the industry through technological developments like IoT led to a vast increase in available data, which allowed AI in the sector to bloom.

---

[45] C Kutterer, 'Regulating Foundation Models in the AI Act: From "High" to "Systemic" Risk' AI Regulation (2024) <https://ai-regulation.com/regulating-foundation-models-in-the-ai-act-from-high-to-systemic-risk/?utm_source=substack&utm_medium=email> accessed 12 February 2024.

[46] Art 52a(3) AI Act.

[47] Chapter VI AI Act.

[48] Chapter VII AI Act.

[49] Chapter IX AI Act.

[50] Chapter XII AI Act.

[51] H Taherdoost, *Thinking Machines: Artificial Intelligence and Machine Learning* in *Innovating and Integrating Emerging Technologies* (Springer 2025) https://doi.org/10.1007/978-3-031-93953-2_5, p 55.

[52] SJ Russell and P Norvig, Artificial Intelligence: A Modern Approach (1st edn, Prentice Hall 1995).

[53] M Trabelsi, E Casprini, N Fiorini, and L Zanni, 'Unleashing the Value of Artificial Intelligence in the Agri-Food Sector: Where Are We?' 125 (2023) *BFJ* 13, 482.

[54] K Ashton, 'How the Term "Internet of Things" Was Invented' in AD Rayome (ed), Tech Republic (2018).

[55] NN Misra, Y Dixit, A Al-Mallahi, MS Bhullar, R Upadhyay, and A Martynenko, 'IoT, Big Data, and Artificial Intelligence in Agriculture and Food Industry' (2020) https://doi.org/10.1109/JIOT.2020.2998584.

https://doi.org/10.1017/err.2025.10058 Published online by Cambridge University Press

In the agrifood context, AI is seen as a technology that could help tend to important and long standing agrifood sectoral values such as food security,[56] food quality management and food safety,[57] food supply chain optimization,[58] food traceability,[59] and sustainability.[60] The impact of AI on food security is expected from its ability to help optimize production practices, enhance decision-making and through improving overall efficiency.[61] Current implementations of AI used for food safety mostly relate to public health monitoring, forecasting preharvest food safety hazards and, to a lesser degree, identifying foodborne pathogens.[62] Food traceability refers to the ability of food companies to trace their products one step back in the supply chain, which is a regulatory requirement under EU law.[63] AI, together with IoT, is argued to synergize with blockchain technologies to increase the reliability and traceability of food items by providing a more reliable way of collecting and entering data in immutable blockchain ledger databases,[64] thereby theoretically solving the utility negating reliance of blockchain technologies on the reliability of entities inputting data, which is called "the oracle problem."[65] AI's advantages for sustainability stem mostly from its ability to improve resource efficiency relating to reducing agricultural inputs such as fertiliser, pesticides and water usage.[66]

The distinction between regular software and AI in agrifood will be apparent in most cases as clear AI methods like machine-learning, reinforcement-learning, deep-learning or knowledge-based systems are often used to accomplish the different functions. An example of regular agrifood software would be a simple program that receives recorded soil humidity levels and that turns on a sprinkler if the humidity level is below a predefined threshold, this could be turned into an AI system by using any of the AI methods above to have the system "predict" or "infer" based on some available farm metrics when the sprinkler needs to turn on, optimising for example growth productivity and water use efficiency.[67]

[56] DK Pandey and R Mishra, 'Towards sustainable agriculture: Harnessing AI for global food security' (2024) Artificial Intelligence in Agriculture https://doi.org/10.1016/j.aiia.2024.04.003, p 73; HU Rahman et al., 'Applications of artificial intelligence (AI) in managing food quality and ensuring global food security' 14 (2024) Journal of Food Safety and Quality 2393287 https://doi.org/10.1080/19476337.2024.2393287, p 8; Kutyauripo (n 1), p 1.

[57] J Rugji et al, "Utilization of AI – reshaping the future of food safety, agriculture and food security – a critical review" (2024) Critical Reviews in Food Science and Nutrition https://doi.org/10.1080/10408398.2024.2430749; K Wang et al, "Advancing food safety behavior with AI: Innovations and opportunities in the food manufacturing sector" (2025) Trends in Food Science & Technology 105050 https://doi.org/10.1016/j.tifs.2025.105050: Rahman (n 48), p 2; C Qian et al, "How Can AI Help Improve Food Safety?" (2023) 14 Annual Review of Food Science and Technology 517 https://doi.org/10.1146/annurev-food-060721-013815.

[58] Pandev (n 56), p 79; Rahman (n 56), p 7.

[59] A Hassoun et al, "Food traceability 4.0 as part of the fourth industrial revolution: key enabling technologies" (2022) Critical Reviews in Food Science and Nutrition 873 https://doi.org/10.1080/10408398.2022.2110033; Rahman (n 56), p 8.

[60] Pandev (n 56), p 78; Rahman (n 56), p 8; M van Hilten et al, "Ethical, Legal and Social Aspects (ELSA) for AI: An assessment tool for Agri-food" 10 (2025) *Smart Agricultural Technology* 100710 https://doi.org/10.1016/j.atech.2024.100710, p 7.

[61] Pandev (n56), p 81.

[62] Ruggi (n 57), p 33.

[63] Art 18 Regulation (EC) No 178/2002 of the European Parliament and of the Council of 28 January 2002 laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety [2002] OJ L 31/1.

[64] A Hassoun et al, "Food Traceability 4.0 as Part of the Fourth Industrial Revolution: Key Enabling Technologies" 64 (2024) *Critical Reviews in Food Science and Nutrition* 873 https://doi.org/10.1080/10408398.2022.2110033.

[65] G Caldarelli, C Rossignoli and A Zardini, "Overcoming the Blockchain Oracle Problem in the Traceability of Non-Fungible Products" 12 (2020) *Sustainability* 2391 https://doi.org/10.3390/su12062391.

[66] Pandev (n 56), p 78; Rahman (n 56), p 8; Van Hilten (n 60), p 7.

[67] H Wei and others, "Irrigation with Artificial Intelligence: Problems, Premises, Promises" (2024) 4 *Human-Centric Intelligent Systems* 187 https://doi.org/10.1007/s44230-024-00072-4, p 190.

In practice, AI techniques have been applied in virtually every level of the agrifood value chain from production to consumption.[68] In plant production computer vision has been used to diagnose diseases in plants in order to manage plant health.[69] Another example is application of pesticides, where a smart sprayer that uses Computer Vision in the form of a convolutional neural network combined with deep learning was used to efficiently apply pesticides to plants.[70] Prediction of yields in production is also a possible using AI, for example an Artificial Neural Network (ANN) was used to predict milk-yield of cows.[71]

AI has also been used in post-production processes of the agrifood system such as food-processing, food safety assessment and quality control, supply-chain traceability and predictive food recommendation.[72] An example of AI used in food-processing and food safety is an intelligent fruit-sorting system utilising a Convolutional Neural Network to separate fresh from rotten fruits.[73] For food traceability, deep-learning methods for predictive assessment, anomaly detection, model optimisation and decision-feedback can be used to provide insights into the supply-chain when integrated together with IoT and blockchain in a perception layer, network layer and application layer structure.[74]

The broad range of technologies that the term "AI" covers under the AI Act means that "AI in agrifood" encapsulates a vast range of systems that can be used in various agrifood processes. The different uses of AI can have a large variety of implications depending on the context and the type of AI technology used. It is therefore useful to highlight some general takeaways about agrifood AI systems that can help understand the degrees of risk in this specific context.

First, agrifood AI promises efficiency gains by optimising production and reducing inputs like chemicals, pesticides, water and energy,[75] generally considered aligning with the idea of sustainability and EU's sustainability agenda.[76] However, it is possible the use of AI could have undesirable effects, for example it could result in an increase in pesticide intensity and toxicity through lowering of costs and through removing humans from the application process.[77]

Second, agrifood AI varies in levels of autonomy. Some systems simply assist decision-making and require a human to act on predictions, like an AI decision-support system for milk yield and animal health,[78] while others could operate with a degree of autonomy, such

[68] Kutyauripo (n 1).

[69] Ozyilmaz U, "Evaluation of the Effectiveness of Antagonistic Bacteria Against Phytophthora Blight Disease in Pepper with Artificial Intelligence" (2020) 151 Biological Control 104379 https://doi.org/10.1016/j.biocontrol.2020.104379.

[70] V Partel, S Charan Kakarla, and Y Ampatzidis, "Development and Evaluation of a Low-Cost and Smart Technology for Precision Weed Management Utilizing Artificial Intelligence" 157 (2019) Computers and Electronics in Agriculture 339–50 https://doi.org/10.1016/j.compag.2018.12.048.

[71] W Grzesiak, P Błaszczyk, and R Lacroix, "*Methods of Predicting Milk Yield in Dairy Cows—Predictive Capabilities of Wood's Lactation Curve and Artificial Neural Networks (ANNs)*" (2006) *Computers and Electronics in Agriculture* https://doi.org/10.1016/j.compag.2006.08.004.

[72] Z Dakhia and others, "AI-Enabled IoT for Food Computing: Challenges, Opportunities, and Future Directions" 25 (2025) Sensors 2147 https://doi.org/10.3390/s25072147.

[73] M el Amin G, S Benkrama and M Bendjima, "Smart Food Sorting Using Deep Learning" (2024) 3rd Int'l Conf on Advanced Electrical Engineering (ICAEE), IEEE https://doi.org/10.1109/ICAEE61760.2024.10783364 accessed 8 May 2025.

[74] RS Alonso and others, "An Intelligent Edge-IoT Platform for Monitoring Livestock and Crops in a Dairy Farming Scenario" 98 (2020) *Ad Hoc Networks* 102047.

[75] S Abbate, P Centobelli and R Cerchione, "The Digital and Sustainable Transition of the Agri-Food Sector" 187 (2023) Technological Forecasting & Social Change 122222 https://doi.org/10.1016/j.techfore.2022.122222, p 7.

[76] HJP Marvin et al, "Digitalisation and Artificial Intelligence for Sustainable Food Systems" 120 (2022) Trends in Food Science & Technology 344 https://doi.org/10.1016/j.tifs.2022.01.020.

[77] Ryan (n. 4).

[78] S Balhara, RP Singh and AP Ruhil, "Data Mining and Decision Support Systems for Efficient Dairy Production" 14(5) (2021) Veterinary World 1258–62 https://www.veterinaryworld.org/Vol.14/May-2021/25.pdf.

as a fruit-picking robots or a food-sorting machine separating ripe, unripe and rotten fruits. Non-autonomous systems can cause harm indirectly through incorrect predictions acted upon by humans, but a human remains in control.

Third, damage potential differs. Embodied AI, controlling devices ranging from small actuators to drones or heavy machinery,[79] can pose direct mechanical risks proportional to the machine's nature, mass and power. Moreover, embodied machines can also pose risks related to faults resulting from when the machine makes an erroneous call that results in damage, like for example not recognizing spoiled food and thus failing to remove it from a conveyor belt.

Finally, complexity levels vary greatly. Some systems rely on single AI models; others use integrated techniques requiring extensive inputs. Greater complexity reduces foreseeability of harmful outcomes, potentially complicating risk-assessments and prevention of harm.

2. *Application of AI Act to agrifood AI*

The following section explores how the AI Act could apply to AI systems deployed in the agrifood domain, to provide non-exhaustive illustrative insights of the relevance and the implications of the AI Act in this sector. To this end, the section analyses how the AI Act's risk categories apply within the agrifood sector by identifying examples of AI systems that correspond to each category based on a review of AI applications in the field. The section analyses the risk categories in the following order: (a) prohibited practices, (b) high-risk systems, and (c) transparency and GPAI requirements.

a. Prohibited practices in the agrifood sector

The AI Act prohibits several types of AI system in Article 5. The list of prohibited AI systems in the AI Act relates in large part to either algorithmic surveillance or law enforcement and those prohibitions are not likely to have far-reaching implications for the agrifood context. However, the prohibitions of AI systems used for manipulation of natural persons and the prohibition of AI systems used to infer emotions could have application to agrifood related AI systems.

*i. Manipulative and deceptive AI systems in AI food recommendation***.** First, the prohibitions on manipulation of natural persons laid out in Article 5(a) of the AI Act prohibits placing on the market of an AI system that "*deploys subliminal techniques beyond a person's consciousness . . . with the objective, or the effect of materially distorting the behaviour of a person or a group of persons by appreciably impairing their ability to make an informed decision.*" Whether subliminal techniques actually work is controversial, but manipulation and deception could certainly be committed through AI.[80] Manipulation can be understood as "distorting the form or structure of the Judgement process, leading to outcomes that may not be in the best interests of the decision maker" and deception can be defined as "producing false information to distort the content of decision-making that may not be in the interest of

[79] K Spanaki et al, "Artificial Intelligence and Food Security: Swarm Intelligence of AgriTech Drones for Smart AgriFood Operations" 33(16) (2022) Production Planning & Control 1498–516 https://doi.org/10.1080/09537287.2021.1882688.; Autonomous robotic weed removal vehicle: PixelFarming Robotics, "*Robot One Brochure*" (2024) https://pixelfarmingrobotics.com/wp-content/uploads/2024/11/Robot-One-Brochure-20241101.pdf accessed 6-11-2024.

[80] H Zhong, E O'Neill and JA Hoffmann, "Regulating AI: Applying Insights from Behavioural Economics and Psychology to the Application of Article 5 of the EU AI Act" in Proceedings of the Thirty-Eighth AAAI Conference on Artificial Intelligence (AAAI-24) (Association for the Advancement of Artificial Intelligence, 2024); M Leiser, 'Psychological Patterns and Article 5 of the AI Act: AI-Powered Deceptive Design in the System Architecture and the User Interface' 1(1) (2024) J AI Law & Regulation 5 https://doi.org/10.21552/aire/2024/1/4.

the decision maker."[81] Imitating, obfuscating, tricking, calculating and reframing are techniques of deception that could potentially be employed by AI systems.[82] "Nudging" can also be seen as a manipulative technique.[83]

Food recommender AI systems are systems based on nutritional informatics supply people with food recommendations based on personal preferences and health data.[84] Such systems can manipulate, deceive or nudge users through food recommendations. Optimal recommendations could be altered by silently incorporating parameters that might not be in the interest of the user, driven by things like profit-optimization or ideological convictions. Such AI food recommendation systems that manipulate, deceive or nudge users, could be considered prohibited under the AI Act.

ii. Emotion recognition for evaluating food consumption. Second, the prohibition of AI systems used to infer emotions of natural persons in the areas of the workplace and educational institutions as laid out in article 5(f) of the AI Act specifically prohibits placing on the market of AI systems that "*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*." This is relevant in the context of evaluation of food consumption, specifically for AI systems that measure the effects of eating on emotions.[85] These AI systems are used in scientific research on nutrition and behaviour, but AI models used solely for scientific research and development are permitted based on Article 1(6) of the AI Act, leaving those systems exempted.

b. High-risk practices in the agrifood sector

The high-risk category found in Article 6 has clear and far-reaching implications for the sector. There are two ways for an AI system to be categorized as high-risk AI (see above). First, when a system is used as a safety component to a device that is required to undergo conformity assessment based on Union harmonisation regulation and second, when an AI system is used in a field, industry or area of application that is considered high-risk because of its nature. This section analyses both in turn.

i. AI as a safety component: Article 6(1). The AI Act categorises an AI system as high-risk when it uses an AI safety component on a system that is, as a whole, required to undergo conformity assessment under one of the EU harmonisation regulations listed in Annex I of the AI Act.

A "*safety component*" is "*a component of a product or of an AI system which fulfils a safety function for that product or AI system, or the failure or malfunctioning of which endangers the health and safety of persons or property*."[86] This alone could be taken to include a vast range of AI systems that have some sort of safety function, for example AI used in food safety. AI can play a vital role in ensuring food hazards such as chemical, physical hazards or food-borne diseases are detected somewhere in the production-chain as to prevent them from being consumed. However, such AI systems are currently not considered high-risk under

[81] Ibid.

[82] P Masters et al, "Characterising Deception in AI: A Survey" in Proceedings of the International Workshop on Deceptive AI (DeceptECAI 2020, DeceptAI 2021), Communications in Computer and Information Science vol 1296 (Springer, 2022) 3.

[83] Ibid.

[84] S Abhari and others, "A Systematic Review of Nutrition Recommendation Systems: With Focus on Technical Aspects" 9(6) (2019) Journal of Biomedical Physics and Engineering 591–602 https://doi.org/10.31661/jbpe.v0i0.1248.

[85] Jacqueline Martinali, "Consumers' food choices and emotions" (Noldus Information Technology, 7 November 2019) <https://www.noldus.com/blog/consumers-food-choices-and-emotions>, accessed 26 November 2024.

[86] Art 3(14) AI Act.

the AI Act, because they are not covered by any of the listed EU harmonisation legislations listed in Annex I.

Two of the EU harmonisation regulations listed in Annex I are relevant for the agrifood context: Regulation (EU) No 167/2013 on the approval and market surveillance of agricultural and forestry vehicles,[87] and the Machinery Regulation.[88]

Through the way in which Article 6(1) is drawn up, the meaning of "safety component" is coloured by the types of equipment or machinery that are covered by the listed EU harmonisation legislations. This likely entails that the meaning of "safety" under the AI Act is not entirely congruent with the meaning of "safety" in other parts of EU law, such as for example the established principle of "food safety" in EU food law.

An example of an AI system that would be covered by one of the listed EU harmonisation legislations is an automated tractor that utilises sensors, cameras and AI algorithms to avoid collisions with persons or obstacles. The safety component would be the AI component of the system that is responsible for ensuring that the tractor does not inflict harm on its surroundings.

Regulation (EU) No 167/2013 is explicitly meant for the agrifood context as it covers tractors, track-laying tractors, trailers and interchangeable towed equipment.[89] This includes vehicles of different sizes, from light tractors weighing less than 600kg,[90] to very large towable trailers with a sum of allowed axle masses that exceed 21.000kg.[91] For the AI Act relevant vehicles that fit this category are, of course, actual tractors that have been automated through AI.[92] However, agricultural or agroforestry vehicles that might not classically look like one of the mentioned vehicles, but that do contain some qualities of such vehicles, could also be covered by Regulation (EU) No 167/2013. Take for example an existing automated weed removal AI system, which essentially consist of a metal, almost square box frame on wheels, with a complete absence of seating for any human controller, packed with sensors, computers and on its underside several robotic arms to remove weeds.[93] Based on its purpose, form and measurements this vehicle could be categorised as either a special purpose wheeled tractor (T4),[94] or an extra-wide tractor (T4.2).[95] Such an autonomous vehicle might still possess enough qualities of a tractor to be considered as such. In fact, it might make sense to say that most agricultural or agroforestry machinery on wheels that resemble one of the mentioned categories is intended to be covered by the regulation, and thus that AI safety components used in such machinery are considered as high-risk under the AI Act.

However, what about vehicles, machines or robots that definitely do not qualify as tractors? Agricultural or food machinery that is not covered by Regulation (EU) No 167/2013 will often still be required to undergo conformity assessment under the Machinery Regulation.[96] "Machinery" is a very broad term that means any powered assembly of linked, movable parts intended for a specific function, including incomplete,

[87] Regulation (EU) 167/2013 of the European Parliament and of the Council of 5 February 2013 on the approval and market surveillance of agricultural and forestry vehicles [2013] OJ L60/1. (hereafter: Regulation (EU) 167/2013).

[88] Machinery Regulation; H Burden, S Stenberg and K Flink, *When AI Meets Machinery – The Role of the Notified Body* (RISE Research Institutes of Sweden 2024) 18.

[89] Art 2 Regulation (EU) No 167/2013.

[90] Art 4(4) Regulation (EU) No 167/2013.

[91] Art 4(14) Regulation (EU) No 167/2013.

[92] A clear example would be an automated actual tractor that can still be steered by a human operator.

[93] Autonomous robotic weed removal vehicle: PixelFarming Robotics, "*Robot One Brochure*" (2024) <https://pixelfarmingrobotics.com/wp-content/uploads/2024/11/Robot-One-Brochure-20241101.pdf> accessed 6-11-2024.

[94] Art 4(5) Regulation (EU) No 167/2013.

[95] Art 4(7) Regulation (EU) No 167/2013.

[96] Art 2(i) Machinery Regulation.

https://doi.org/10.1017/err.2025.10058 Published online by Cambridge University Press

installed-on-site, combined, lifting-only or software-dependent assemblies.[97] This includes both machinery from the agricultural and the more food related contexts, such as harvesting robotics, as well as food processing and sorting machinery and others. AI safety components used in such machinery would also be considered high-risk under Article 6(1) of the AI Act. An example of a machine that could fall on the non-tractor side of the definition of "tractor" could be a driving box on wheels that uses several drones, connected to it with electrical and data cables, to pick fruits or vegetables.[98] Another example would be an AI driven food-sorting machine using an AI component that prevents harm to factory personnel. Such machines are covered by the Machinery Regulation and thus, if they were to use an AI safety component, this component would be considered high-risk under the AI Act. Another example is an indoor farming system controlled with AI that uses a 3D-printer-like setup with camera sensors and AI algorithms to manage the insides of a greenhouse. Other types of machinery used in, for example, food-processing would also qualify.

Besides applicability of the AI Act to machines covered by the Machinery Regulation, the Machinery Regulation also has its own rules for safety components that use machine learning. All safety components of machinery with "fully or partially self-evolving behaviour using machine learning approaches" must undergo either EU type-examination and third party conformity assessment, full quality assurance, or unit verification.[99] "Self-evolving" in this respect relates to how some systems, during their operations, update how they work, which can lead to unforeseeability and uncertainty about their abilities of avoiding harm. Not all AI systems "learn" on the job, there are also systems that have a level of "intelligence" but that do not continuously update while they work. Actively "learning" safety components, which inevitably fit the definition of AI under the AI Act, must undergo a third-party conformity assessment under the Machinery Regulation and would thus be automatically considered high-risk under Article 6(1) of the AI Act. What this essentially means is that safety components that actively "learn" that are used in machinery covered by the Machinery Regulation have to comply not only with the requirements for "self-learning" systems under the Machinery Regulation, but also with the requirements for high-risk AI systems under the AI Act.[100]

ii. Areas of AI application that are high-risk based on their context: Article 6(2). Next, AI systems listed in Annex III of the AI Act are always considered high-risk because of the context in which the system operates. The agrifood context is not explicitly listed there. AI systems managing "*critical infrastructure*" are labelled as one of the high-risk areas of application as listed in Annex III (2), but the wording of in Annex III (2) does not include the food system: "*Critical infrastructure: AI systems intended to be used as safety components in the management and operation of critical digital infrastructure, road traffic, or in the supply of water, gas, heating or electricity*." A literal reading of Annex III (2) therefore entails that it does not cover the food system and the food system is therefore not a high risk area of application under the AI Act.

Stepping outside of the risk-categorisation system for a moment: the text of the AI Act could raise some confusion, as the AI Act has a general wider definition for "*critical infrastructure*" that can include certain parts of the food system, as will be shown in the next paragraphs. The relevance of this broader definition is that the AI Act contains

[97] Art 3(1) Machinery Regulation.

[98] Autonomous fruit harvesting vehicle: Tevel, "*Technology*" (Tevel Tech, 2024) <https://www.tevel-tech.com/technology/> accessed 6 November 2024.

[99] Art 25(2), Annex II, Annex VII, Annex VIII, Annex IX and Annex X of the Machinery Regulation.

[100] Burden (n 88).

reporting duties for "*a serious and irreversible disruption of the management or operation of critical infrastructure*".[101]

Article 3 (62) of the AI Act contains the following definition: "*Critical infrastructure: means critical infrastructure as defined in Article 2, point (4), of Directive (EU) 2022/2557*." "*Critical infrastructure*" as defined in Article 2, point (4) of Directive (EU) 2022/2557 means "*an asset, a facility, equipment, a network or a system, or a part of an asset, a facility, equipment, a network or a system, which is necessary for the provision of an essential service*." "*Essential service*" as defined in Article 2, point (5) of Directive (EU) 2022/2557 means "*a service which is crucial for the maintenance of vital societal functions, economic activities, public health and safety, or the environment*."

Directive (EU) 2022/2557 entails that Member States must identify "*critical entities*" for the sectors listed in the Annex of the Directive that provide one or more "*essential services*" and that operate "*critical infrastructure*" located in the Member State territory.[102] Point 11 in the Annex contains "*Production, processing and distribution of food*" as a listed sector and it references as entities that can be designated as "*critical entities*" the following: "*Food businesses as defined in Article 3, point (2), of Regulation (EC) No 178/2002 of the European Parliament and of the Council (22) which are engaged exclusively in logistics and wholesale distribution and large scale industrial production and processing*."

Since such businesses can be designated as "*critical entities*" by Member States under Directive (EU) 2022/2557 and because "*critical entities*" can only be designated if they provide one or more "*essential services*" and if they operate "*critical infrastructure*" located on that Member State territory, the infrastructure that "*Food businesses … which are engaged exclusively in logistics and wholesale distribution and large scale industrial production and processing*" operate, i.e. crucial parts of the food system, must at least have the potential to be "*critical infrastructure*" as understood in the context of Directive (EU) 2022/2557.[103] Because the definition of "*critical infrastructure*" under the AI Act is linked to the definition of Directive (EU) 2022/2557 through Article 3 (62) of the AI Act, the infrastructure that aforementioned entities would operate, i.e., parts of the food system, can also be "*critical infrastructure*" in the context of Article 3 (62) of the AI Act.

However, what is crucial to note here once more is that not all types of '*critical infrastructure*' covered by Directive (EU) 2022/2557 are labeled as high risk under the AI Act. Only certain types of "*critical infrastructure*" from the broad definition found in Article 3 (62) are classified as high risk under Annex III (2):"*AI systems intended to be used as safety components in the management and operation of critical digital infrastructure, road traffic, or in the supply of water, gas, heating or electricity*."[104] Therefore, since Annex III (2) does not mention the food system, AI systems managing parts of the food system are not classified as high risk on a literal reading of the AI Act.

c. Transparency and GPAI in the food sector

Lastly, the risk category concerning transparency is a very broad open category that certainly does have application to the agrifood context. However, the implications of the AI Act's special rules on transparency likely mostly relate to non-sector specific questions, such as being subjected to AI while in employment or AI used in marketing.

[101] Article 3 (49b), 26(5), 55(1c), 60(7), 73 AI Act.

[102] Article 6(2) Directive (EU) 2022/2557.

[103] CM Galanakis and others, "Landscape of Policies, Standards, Approaches, and Projects for EU Food Security: An Overview" (2025) Discover Food (Review article, accepted 8 April 2025) <https://link.springer.com/journal/44297> (forthcoming).

[104] Annex III (2) AI Act.

Transparency requirements based on Article 50 of the AI Act would for example be applicable to AI human resource management (HRM) systems used to optimize agrifood workers productivity.[105] Another example of a system that should come with transparency about its use would be generative AI used in food-marketing.

Turning to GPAI, it is unlikely that the agrifood sector will produce such models, since their creation requires extensive computation and vast multi-domain datasets. However, companies in the agrifood sector may fine-tune and adapt existing GPAI models. Applying the logic of high-risk AI systems to GPAI would mean that when this fine-tuning is considered a "*substantial modification*," which means it is a modification that results in consequences not foreseen in the initial conformity assessment by the initial provider, the person conducting the fine-tuning becomes the provider himself and should comply with the requirements laid out for high-risk AI systems.

d. Summary

This section provided a high-level overview of how the AI Act could be relevant to AI systems in the agrifood system. The AI Act has several clear implications for AI in the agrifood sector:

a. There are some prohibited practices that could arise in the agrifood context although this might not be a vast amount. Manipulation through food recommendation and emotion recognition during eating were highlighted here as examples, but there might be more prohibited practices that could arise in the agrifood context.
b. More pronounced implications arise as a result of the high-risk categorisation of AI safety components in agrifood machinery and equipment covered by Regulation (EU) No 167/2013 on the approval and market surveillance of agricultural and forestry vehicles and the Machinery Regulation. This includes a large range of AI agricultural and food equipment that will have some AI mechanism for ensuring safety to the people around the machine.
c. Although included in the definition of "*critical infrastructure*" read in conjunction with Directive (EU) 2022/2557 on the resilience of critical entities, AI systems managing parts of the food system are not classified as high risk because Annex III (2) of the AI Act does not list it.
d. Next, two examples of AI systems with special transparency requirements were provided, namely AI employee management and food advertising, as to highlight in what types of contexts such requirements apply.
e. Lastly, the rules of the AI Act on GPAI do not seem to raise immediate concerns for agrifood practitioners, since it is unlikely that the sector will produce GPAI, and the AI Act does not contain requirements for users of GPAI.

4. An agrifood perspective on the AI Act

While the AI Act establishes a clear risk categorisation system, the agrifood context might present sector-specific nuances and challenges that are potentially less well addressed in the generally applicable AI Act. The agrifood-sector specific challenges discussed here pertain to: (a.) potential implications of AI for food security, (b.) to how extensive the term

[105] Y Zhai, L Zhang, and M Yu, "AI in Human Resource Management: Literature Review and Research Implications" (2024) Journal of the Knowledge Economy https://doi.org/10.1007/s13132-023-01631-z.

"AI safety component" is interpreted, and (c.) to considerations for nonhuman values. This section briefly explores these dimensions.

1. Food security

The use of AI in the agrifood value chain is mostly seen as a beneficial development for food security.[106] However, AI systems can have certain attack and risk vectors and can be undermined under certain conditions.[107] Reliability of AI systems in agrifood is important, especially if the AI systems substantially affects parts of food production, as hacking or malfunctioning could leave AI systems incapacitated, or result in damaged produce, animals and vegetation, or in disabled food supply chains.

As discussed in section III.2.b., the AI Act does not categorize AI systems managing substantial or critical parts of the food system as high risk, because the sector is not listed in Annex II as high-risk critical infrastructure below, the argument is presented that the food system *could* have been included as high-risk "*critical infrastructure*" in Annex II, in particular in the light of the "critical status" it is given in other legal instruments.

For the other parts of the regulation, the AI Act's definition for "*critical infrastructure*" does include parts of the food system.[108] One of the sectors in which Member States can designate entities as "*critical entities*," in the third column of the table in the Annex to Directive (EU) 2022/2557, is: "*Food businesses … which are engaged exclusively in logistics and wholesale distribution and large scale industrial production and processing*." The Recitals of Directive (EU) 2022/2557 clarify that "*critical entities should only be identified among food businesses, whether for profit or not and whether public or private, that are engaged exclusively in logistics and wholesale distribution and large-scale industrial production and processing with a significant market share as observed at national level*."[109] The Directive effectively allows Member States to designate such businesses as regulated critical infrastructure operators holding them to carry out certain risk-assessment and mitigation strategies.

The reasoning behind the effective designation of such businesses as critical infrastructure operators could just as well be applied to AI systems managing such infrastructure, which would result in their development undergoing the scrutiny necessary to prevent or mitigate systemic risks to critical food infrastructure and ultimately to food security. In a similar manner to the Member State discretion of Directive (EU) 2022/2557, the high-risk classification could be made to only apply to designated AI systems managing "*logistics and wholesale distribution and large-scale industrial production and processing with a significant market share as observed at national level*."

Threats to food security are generally taken seriously under EU law, as can be seen in another Directive, Directive (EU 2022/2555 on measures for a high level of cybersecurity.[110] This Directive holds no special significance in relation to the AI Act, but can nonetheless be seen as an indication that threats to critical food infrastructure are

[106] A Ikram and others, "Applications of Artificial Intelligence (AI) in Managing Food Quality and Ensuring Global Food Security" 22 (1) (2024) CYTA – Journal of Food 2393287; A Ahmad and others, "AI Can Empower Agriculture for Global Food Security: Challenges and Prospects in Developing Nations" 15 (2) (2024) International Journal of Agricultural Science 123–45.

[107] K Hartmann and C Steup, "Hacking the AI—The Next Generation of Hijacked Systems" in T Jančárková and others (eds), 20/20 Vision: The Next Decade, Proceedings of the 12th International Conference on Cyber Conflict (NATO CCDCOE Publications 2020), p 335.

[108] Through Article 3 (62) of the AI Act, which refers to Directive (EU) 2022/2557 on the resilience of critical entities for the definition of "*critical infrastructure*," see discussion in section III.2.b.

[109] Recital (5) Directive (EU) 2022/2557.

[110] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) [2022] OJ L333/80.

taken seriously under EU law. Similar to Directive (EU) 2022/2557, this Directive also labels food businesses engaged in wholesale distribution and industrial production and processing as critical entities operating in a critical sector. Under Directive (EU) 2022/2555, medium-sized or larger operators conducting food-supply activities, and smaller ones whose failure would jeopardise supply, automatically fall within scope as "*important entities*,"[111] which means they have cybersecurity-risk management and incident-notification duties.[112]

It is somewhat peculiar that cybersecurity risk-management is required from critical food infrastructure operators, but AI systems operating the same infrastructure are not subject to the risk-management scrutiny that comes with the high-risk classification under the AI Act. The exclusion of critical food supply chains from the high-risk classification as it currently stands in the AI Act could present a gap that could pose a threat to EU food security. Future research could explore whether the AI Act, without the high-risk classification of AI systems managing crucial food infrastructure, properly addresses the core EU food law principle of food security.

2. "Safety components" in the context of agrifood safety

The AI Act intends to address safety through the high-risk categorisation of certain AI safety components. However, it is currently not entirely clear how extensively the meaning of "safety" must be understood in this context. To reiterate a "*safety component*" is "*a component of a product or of an AI system which fulfils a safety function for that product or AI system, or the failure or malfunctioning of which endangers the health and safety of persons or property*."[113] However, an AI safety component is only high risk under the AI Act when it is used on a product covered by one of the Union Harmonisation Regulations listed in Annex I. The meaning of "safety component" under the AI Act can therefore be understood to relate only to the types of safety hazards that are contextual to the types of products covered by the listed Union Harmonisation Regulations.

The agrifood relevant Regulation (EU) No 167/2013 on the approval and market surveillance of agricultural and forestry vehicles and the Machinery Regulation seem to relate mostly to safety in relation to mechanical hazards.[114] While mechanical hazards are the most common source of injury in agriculture,[115] there are more agricultural and food related health and safety concerns that might be affected by AI (safety) components. The question can be raised whether AI safety components dealing with non-mechanical safety hazards such as food safety, that are also covered by one of the Union Harmonisation Regulations like the Machinery Regulation, are also "safety components" for the purposes of the AI Act. The answer could have relevant implications for the agrifood context, where food safety is considered a crucial paradigm.[116]

In food safety, AI can play a vital role in detecting food hazards and failure of such AI systems could have detrimental consequences. An embodied AI system used for fruit sorting that separates fresh and rotten fruits certainly is machinery covered by the

[111] Art 2 Directive (EU) 2022/2555.

[112] Chapter IV Directive (EU) 2022/2555.

[113] Art 3(14) AI Act.

[114] See, for example, the indicative list of safety components in Annex II of the Machinery Regulation.

[115] R Jadhav, C Achutan, G Haynatzki, S Rajaram and R Rautiainen, "*Review and Meta-analysis of Emerging Risk Factors for Agricultural Injury*" 21 (3) (2016) Journal of Agromedicine 284–97 https://doi.org/10.1080/1059924X.2016.1179611, p 1.

[116] See, for example, the General Food Law Regulation: Regulation (EC) 178/2002 of the European Parliament and of the Council of 28 January 2002 laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety [2002] OJ L31/1; Ruggi (n 60).

Machinery Regulation.[117] When that system fails to detect rotten fruit, that rotten fruit can become a food safety hazard. Does the fact that this AI system used in machinery is a component autonomously affecting food safety make it a "safety component" under the AI Act?

An AI system like this poses a non-mechanical risk and it is not entirely clear whether this risk is an intended safety concern covered by the meaning of "safety component" under the AI Act and the Machinery regulation. The indicative list of Annex II of the Machinery Regulation suggests this is not the case.

In this respect, it does seem reasonable to limit to an extent the types of safety that a developer of an AI safety component must address, as what is foreseeable for a developer in terms of safety implications is understandably not endless. However, it is currently not entirely clear where the limit lies and whether, for example, food safety falls within the regulatory scope.

Since it is ultimately the EU harmonisation regulation that is used to scope the high-risk categorisation of AI safety components under the AI Act, the rationale of the inclusion of the specific EU harmonisation regulation is likely significant for how extensive the meaning of "safety" must be understood in that context.

AI safety components used in machinery that is required to undergo a conformity assessment under the Machinery Regulation are high risk AI under the AI Act. If non-mechanical types of safety, such as food safety, are not intended to be covered by the Machinery Regulation, then AI driven machinery that directly affects food-safety is not high-risk under the AI Act. This would mean the risks to food safety that such an AI system poses would only be addressed through other legal schemes such ass ex-post liability through, for example, the Product Liability Directive. This could present a gap in risk prevention and mitigation that could be explored further to ensure comprehensive regulatory coverage.

3. Non-human and "sustainability" values

The AI Act was made with a human-centric approach.[118] The agrifood context is typically marked by (some) concern for risks to non-human values, some of which are in the sector typically understood as "sustainability" values such as the environment, animal welfare and biodiversity. This section highlights that such non-human values are not extensively covered by the AI Act and this could be regarded to constitute a gap in the legal framework from the perspective of the agrifood context.

Article 1 of the AI Act delineates that the purpose of the AI Act is "*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*." The environment is mentioned here, but as will be shown below, this appears to be largely rhetorical and limited in its implications. Recital (6) provides some further explanation of human-centric: "*As a prerequisite, AI should be a human-centric technology. It should serve as a tool for people, with the ultimate aim of increasing human well-being*."

Scholars had already noted during the early drafting stage of the AI Act that the Act did not materially address environmental values.[119] This has not changed significantly with

[117] El Amin (n 73).

[118] Art 1 AI Act.

[119] U Pagallo, J Ciani Sciolla and M Durante, "The Environmental Challenges of AI in EU Law: Lessons Learned from the Artificial Intelligence Act (AIA) with its Drawbacks" 16 (3) (2022) Transforming Government: People, Process and Policy 359.

the final version of the AI Act. The environment is currently not part of the risk-categorisation system and is mentioned only incidentally throughout the AI Act.

The environment is included in the AI Act in four incidental ways. First, there are several reporting duties for when high-risk AI causes serious incidents including serious harm to the environment.[120] Second, a Member State market surveillance authorities may provide a preliminary authorisation of a high risk AI system while the conformity assessment is still in progress for exceptional reasons, one of which is "*environmental protection*."[121] Third, the quality of the environment, biodiversity, green transition measures and climate change mitigation are reasons of substantial public interest form justifications for the processing of personal data in regulatory sandboxes[122] Fourth and last, environmental sustainability and energy-efficient programming are given as an example of values that can be part of the voluntary codes of conduct that can be drawn up for the industry.[123]

Contrastingly, biodiversity is mentioned only once incidentally, and animal welfare is not mentioned at all. AI is certainly expected to have an impact on animal welfare, with literature highlighting potential positive impacts such as better living conditions and more individual treatment of animals,[124] as well as potential negative impacts like increased objectification of animals.[125]

The human-centric approach of the AI Act results in a regulatory document that takes little note of non-human values. These values can be substantially affected by AI in the agrifood sector. As a result of not including non-human values such as the environment, animal welfare and biodiversity in the risk-categorisation system, there could be a potential these values are compromised by agrifood AI technologies.

5. Conclusion

This article set out to explore how the AI Act's risk-categorisation system applies to AI in the agrifood sector, addressing the opportunities and challenges of regulating emerging technologies in this critical domain.

The analysis began with an overview of the AI Act, focusing on its definition of AI, its risk-categorisation system, and the requirements for high-risk AI systems. Next, the article examined the application of AI in the agrifood sector, offering a non-exhaustive categorisation of agrifood AI systems under the AI Act's framework. Some examples of prohibited AI and AI with special transparency were highlighted. Most attention went to the high-risk categorisation for AI safety components used in agrifood machinery, as this can be expected to have extensive implications for the agrifood sector. While parts of the agrifood system can be "*critical infrastructure*" in the broad definition of the AI Act, AI systems managing such systems are not categorised as high-risk as they are not listed in Annex II. The rules for GPAI will likely not have strong implications for the agrifood sector as it is unlikely that the sector will develop GPAI. Finally, the article highlighted several concerns that remain unaddressed by the current regulatory regime.

The first concern relates to the exclusion of AI systems managing critical food infrastructure covered by Directive (EU) 2022/2557. These are not high risk under the AI Act, but perhaps they should be, as they could potentially pose a threat to food security.

[120] Art 3(49), 26(5), 55(1c), 60(7), 73 AI Act.

[121] Art 46(1) AI Act.

[122] Art 59 AI Act.

[123] Art 95 (2b) AI Act.

[124] L Zhang et al, "Advancements in artificial intelligence technology for improving animal welfare: Current applications and research progress" (2023) Animal Research Open https://doi.org/10.1002/aro2.44.

[125] Van Hilten (n 60), p 8.

Next, the scope of "*safety component*" might not include non-mechanical hazards in the agrifood context, which could leave agrifood values like food safety and environmental safety exposed. Lastly, the AI Act does not address sustainability values such as the environment, biodiversity and animal welfare, which could present a regulatory gap.

These open challenges justify closer examination as we progress through the innovation and adoption cycles of AI. Future scholarship into the former are necessary for reaping the benefits of AI while preventing the harms. Both the risks of overinclusion and under inclusion could have negative impacts and risk-benefit analyses are therefore desirable when thinking about the risk system of the AI Act. An example could be to forego the potential classification as high risk of AI safety components in agrifood chemical applicators because of their potential benefits to the sustainability of the sector. Achieving the right assessment of risks will require deep inquiry, an open mind and a forward-looking perspective. Through such efforts, future research can contribute to the development of an even more robust and adaptive risk governance framework for AI in agrifood, one that fosters innovation while realizing the sustainability and resilience of EU food systems.

Funding Statement. Open access funding provided by Wageningen University & Research.

Competing interests. The author has no conflicts of interest to declare.

Cite this article: IL Val, "The EU AI Act and the Food System: How the European Union Ai Act Applies to Agrifood". *European Journal of Risk Regulation.* https://doi.org/10.1017/err.2025.10058