Chapter 2: Prohibited AI Practices

Prohibited AI Practices under the EU AI Act

Patricia García Majado

I. Summary of Art. 5 of the AIA

The European Artificial Intelligence Act (AIA) regulates AI practices based on the levels of risk that they pose to the Union's fundamental rights and values such that, as recital 26 of the preamble states, 'the approach should tailor the type and content of such rules to the intensity and scope of the risks that AI systems can generate'. AI practices categorized as posing an unacceptable risk are therefore those that cannot be used without risking fundamental rights and values of the European Union (art. 5 AIA). This is the basis for their prohibition. Recital 28 of the preamble is the first point in the text we are concerned with where it mentions such practices, stating that despite AI's many beneficial uses, 'it can also be misused and provide novel and powerful tools for manipulative, exploitative and social control practices. Such practices are particularly harmful and abusive and should be prohibited because they contradict Union values of respect for human dignity, freedom, equality, democracy and the rule of law and fundamental rights enshrined in the Charter, including the right to non-discrimination, to data protection and to privacy and the rights of the child'.

The European legislators are making a presumption *juris et de jure* with this point, understanding that certain practices—as configured in the Act itself—are not, at present, susceptible to a legally beneficial use in current European democratic systems, or at least a use that is not detrimental to individuals' fundamental rights. To the extent that it is the legislators themselves who have made this assessment of risk, not certain subjects *a posteriori* in a given case, the AIA can be said to have established a top-down approach to risk[1]. Hence, art. 5 AIA in some way outlines the legal frontiers of AI within the Union; something that was certainly considered necessary from both a legal scholarship and institutional point of view from the very moment that the proposed

[1] De Gregorio, G., & Dunn, The European risk-based approaches: Connecting constitutional dots in the digital age, Common Market Law Review, 2022, 473.

Act was published by the European Commission[2]. I use the term legal frontier not only because the article clearly excludes certain practices, but because art. 5 AIA in some way sets out the scope of high risk systems: AI systems that do not fall within the prohibition are often categorised as high risk and therefore subject to special controls and guarantees.

The need for art. 5 AIA was, however, accompanied by deep consideration. As the basic objective is the protection of subjects' fundamental rights and the values of the Union, legislators also strove to avoid excessive, unnecessary prohibitions. The very first section of the preamble indicates that the objective of the Act is both to 'improve the functioning of the internal market by laying down a uniform legal framework' and, 'ensuring a high level of protection of health, safety, fundamental rights as enshrined in the Charter of Fundamental Rights of the European Union (the 'Charter'), including democracy, the rule of law and environmental protection, to protect against the harmful effects of AI systems in the Union, and to support innovation'. And 'more prohibition' does not, at least not necessarily, mean 'better regulation', nor therefore does it mean more effective protection of individuals' fundamental rights. Certain fundamental rights can also be exercised via artificial intelligence (such as, for example, the right to artistic creation), while it can safeguard others (such as AI systems in public safety or in healthcare, etc.). In short, it means finding a delicate balance between two extremes. Art. 5 AIA is the expression of a considered, albeit not always simple, consensus.

The provision concerning us comes into force on 2 February 2025 (art. 113 AIA), which is before the date specified for the Act as a whole to come into force (2 August 2026). Hence, recital 179 of the preamble states, 'while the full effect of those prohibitions follows with the establishment of the governance and enforcement of this Regulation, anticipating the application of the prohibitions is important to take account of unacceptable risks and to have an effect on other procedures, such as in civil law'.

The purpose of the following pages is not to make a point-by-point examination of each prohibited AI practice, but rather to offer a series of general reflections on art. 5 AIA that will help to understand its meaning and highlight potential shortcomings. After analysing the legislative origin of art. 5 AIA, its object (introduction in the market, making available, and use) will be examined, as will the prohibitions unrelated to art. 5 AIA that also affect various AI systems, the different types of prohibitions (absolute and relative) that the article establishes, and finally, the limited restrictive scope of the provision.

[2] 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, 21 April 2021, available at: https://artificialintelligenceact.eu/wpcontent/uploads/2021/08/The-AI-Act.pdf.

II. The legistlative gestation of Art. 5 AIA: What was there initially and what was not

Precisely because art. 5 AIA expresses—as already noted—the difficult balance between protection of fundamental rights and values of the Union and innovation, it was one of the most hotly-debated provisions of the legislation, and therefore among the provisions with the most changes from its initial wording. The legislative process of art. 5 AIA was, in general terms, progressively restrictive, attempting to provide increasing guarantees. Although various actors were involved in the legislative process, it was the European Parliament[3] that made the most, and the most restrictive, amendments to the original text proposed by the Commission, rather than the Council of the European Union[4]. However, it is also worth noting that the process was influenced by opinions and rulings from various institutional actors, albeit ones without legislative power, such as the European Supervisor of Data Protection, the European Data Protection Board, the Economic and Social Committee, etc., along with other non-institutional actors, basically from the third sector (such as Algorithmic Watch, EDRi, Access Now, etc.), who played an important role in safeguarding the Union's fundamental rights[5].

On the one hand, the Act that was finally passed ended up including more prohibitions than were originally considered. The proposed legislation from the Commission generally prohibited manipulative subliminal AI techniques, those that aim to take advantage of specific vulnerable groups, certain social scoring systems, and certain remote real time biometric identification systems in publicly accessible spaces for law enforcement purposes. The initial proposal did not ban biometric categorization systems, facial recognition databases, emotion recognition systems, or police predictive systems for individuals which were subsequently included—albeit with various modifications and limitations—thanks to various amendments introduced by the European Parliament (amendments 224-227), while the Council only proposed amendments to already established prohibitions, without adding any new bans. The additional prohibitions, however, were also advised or suggested by the European Data Protection Supervisor,

[3] Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)), available at: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html (last accessed on 2 January 2025).

[4] Council of the EU, Presidency Compromise Text (2021/0106(COD)) (29 Nov. 2021), available at: https://data.consilium.europa.eu/doc/document/ST-14278-2021-INIT/en/pdf (las accessed on 2 January 2025).

[5] See, for example, the report: 'An EU Artificial Intelligence Act for Fundamental Rights. A Civil Society Statement', 2021, signed by 123 European and international organizations. Available at: https://edri.org/wp-content/uploads/2021/12/Political-statement-on-AI-Act.pdf.

the European Data Protection Board,[6] and by the Economic and Social Committee,[7] and also highlighted by other non-institutional actors, who criticized the excessive laxity of the original art. 5 AIA[8].

In addition, this progressive restriction was also apparent in the reinforcement or expansion of already established prohibitions. This is because either the *subjective* scope of the prohibition was expanded or—more commonly—because the *objective* scope was expanded. With regard to the former, see, for example, how in the original Commission text, social scoring systems were prohibited when used by public authorities, while in the final Act, that distinction was removed—as proposed by the Parliament and by the European Council—prohibiting such systems from use by both public authorities and strictly private bodies. This is because private bodies introducing such systems in the market, putting them into service, or use can, in certain circumstances, also harm fundamental rights.

The expansion of the objective scope of the prohibitions may be illustrated by the case of manipulative AI techniques. The Commission proposal prohibited an 'AI system that deploys subliminal techniques beyond a person's consciousness', understood as those that use 'audio, image, video stimuli that persons cannot perceive, as those stimuli are beyond human perception' (recital 29). However, because manipulation is not only at the subliminal (imperceptible) level, but also at the liminal, the final Act also prohibited practices that used 'purposefully manipulative or deceptive techniques, 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 (...)'—as proposed by Parliament (amendment 215)—as people in such cases 'can still be deceived or are not able to control or resist them' (recital 29). For instance, consider a chatbot that is used to get people to reveal their passwords.

There was a similar expansion for AI systems that use techniques exploiting people's vulnerabilities. The Commission's proposal prohibited any 'AI system that exploits any of the vulnerabilities of a specific group of persons due to their age, physical or mental disability, in order to materially distort the behaviour of a person pertaining to that group (...)', whereas the vulnerabilities covered by the final text were broadened to include those arising from a 'specific social or economic situation' –'such as persons living in extreme poverty, ethnic or religious minorities', as the preamble states in recital 29—

[6] EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18 June 2021, available at: https://artificialintelligenceact.eu/wp-content/uploads/2022/05/AIA-EDPBEDPS-Opinion-18-June-21.pdf. See pp.2 and 3 for proposed prohibitions from these institutions.

[7] Opinion, European Economic and Social Committee, AI Regulation (INT/940 – EESC-2021-02482-00-00-AC-TRA (EN) 5/8) available at: https://artificialintelligenceact.eu/wp-content/uploads/2022/05/AIA-EESC-Opinion-22-Sept-21.pdf. See section 4.8 which specifies the AI practices that they think should be prohibited.

[8] See note 6.

which now seems to be aimed at covering any reason for discrimination (art. 21 CDFUE).

Although the legislative process of art. 5 AIA generally contributed to expanding its object of regulation, it is also important to emphasize that some of the more restrictive amendments to its initial wording, proposed in particular by the European Parliament, were not accepted. This was no doubt on the understanding that they would mean excessive prohibition that would hinder the achievement of certain objectives that were also important for the Union. One such case involves police predictive systems. The European Parliament proposed prohibiting any 'AI system for making risk assessments of natural persons or groups thereof in order to assess the risk of a natural person for offending or reoffending or for predicting the occurrence or reoccurrence of an actual or potential criminal or administrative offence based on profiling of a natural person or on assessing personality traits and characteristics, including the person's location, or past criminal behaviour of natural persons or groups of natural persons' (amendment 224). It was only to be expected that this proscription would be made more flexible bearing in mind the interests of various member states that already used these types of predictive policing tools for security purposes[9]. And in fact, the current prohibition applies only to *individual* predictive policing systems based solely on creating a profile or evaluation of personality traits, which has watered down Parliament's initially proposed ban.

There was a similar process for remote real-time biometric identification systems, as once again, the European Parliament proposed—unsuccessfully—prohibiting all use of such systems without exception in all settings (amendment 220), not only those related to law enforcement. The same was true for Parliament's proposal to also prohibit 'AI systems for the analysis of recorded footage of publicly accessible spaces through 'post' remote biometric identification systems, unless they are subject to a pre-judicial authorisation in accordance with Union law and strictly necessary for the targeted search connected to a specific serious criminal offense as defined in Article 83 (1) of TFEU that already took place for the purpose of law enforcement', which also ultimately failed to be adopted (amendment 227).

Although, as noted above, the legislative process dealt with many of the main defects in the original art. 5 AIA, it is important to mention others that remained, despite—in certain cases—being expressly highlighted by various actors or by legal scholars. In some cases the scope of application that European legislators have finally opted for is questionable. In other words, in some cases in art. 5 AIA it is difficult to understand—or at least difficult to find explanations to judge the reasoning, fundamentally in the preamble, for the same scope prohibiting certain AI systems but not others.

[9] This had already been predicted by some authors such as Presno Linera, La propuesta de Ley de Inteligencia Artificial Europea, Revista de las Cortes Generales, 2023, 81, p.108.

Without attempting to be exhaustive, and solely as an example, we might mention emotion recognition systems, which are prohibited in the workplace and in education. Recital 44, after noting that expression of emotions varies culturally, and even in the same person, emphasizes 'limited reliability, the lack of specificity and the limited generalisability'. It then goes on to explain that, 'considering the imbalance of power in the context of work or education, combined with the intrusive nature of these systems, such systems could lead to detrimental or unfavourable treatment of certain natural persons or whole groups thereof'. That being the case, it is difficult to fathom why this limited reliability is only a valid reason for excluding such systems in employment and education, because if they are not scientifically reliable, or are highly inaccurate, they may produce harmful results in other contexts as well. Furthermore, the imbalance of power that the legislators note as justifying the prohibition—which is a perfectly valid argument, like the previous one—occurs not only in education and employment, but also in other, even more asymmetrical settings, such as migration and law enforcement, contexts that the European Parliament specifically did attempt to include in the prohibition (amendment 226)[10].

Another example could be real-time remote biometric identification systems, which are only prohibited when used for law enforcement purposes[11], with exceptions laid out in art. 5.1h) AIA. Recital 32 in the preamble explains that such systems, in addition to seriously impinging on people's rights and liberties, 'to the extent that it may affect the private life of a large part of the population, evoke a feeling of constant surveillance and indirectly dissuade the exercise of the freedom of assembly and other fundamental rights', also have technical inaccuracies that 'can lead to biased results and entail discriminatory effects', especially 'with regard to age, ethnicity, race, sex or disabilities'. The preamble continues, 'the immediacy of the impact and the limited opportunities for further checks or corrections in relation to the use of such systems operating in real-time carry heightened risks for the rights and freedoms of the persons concerned (...)'.

In this regard, and in line with what was noted previously, we might ask ourselves whether this feeling of mass vigilance and dissuading effect on the exercise of fundamental rights, the discriminatory bias in the results, and the difficulty of making instant corrections do not also mean that real-time remote biometric identification systems

[10] This was also noted by Díaz González, Prohibited Artificial Intelligence Practices (Article 5), in Huergo Lora and Díaz González (Eds.), The EU Regulation on Artificial Intelligence: A Commentary, 2025 (forthcoming); Carlon, Las Administraciones Públicas ante la Inteligencia Artificial, 2025, p. 77. In addition, Smuha, N., Ahmed-Rengers, E., Harkens, A., Li, W., MacLaren, J., Piselli, R., Yeung, K., How the Eu can achieve legally trustworthy AI, LEADS Lab University of Birmingham, 2021, p. 27, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3899991 proposed prohibition, based on those arguments, in law enforcement.

[11] According to recital 46 AIA, 'law enforcement means activities carried out by law enforcement authorities or on their behalf for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and preventing threats to public security'.

pose an unacceptable risk to fundamental rights and values of the Union in settings other than mere compliance with regulations, such as border control and migration, public security, and healthcare. And of course, whether the same risks are not created when such systems are used by autonomous private actors, not only by public authorities[12]. Once again, these risks are not exclusive to a law enforcement setting.

Legal scholars proposed that the prohibition be extended to all situations where there is some kind of coercion of the individual[13], or more ambitiously, in any setting, as the European Parliament proposed (amendment 220), along with the European Data Protection Supervisor[14]. That does not mean that such systems necessarily be prohibited in these arenas, but instead, it underlines the inconsistency of the European legislators, foreseeing an unacceptable general risk of these systems but then limiting the prohibition of them to a single area. Perhaps it would have been useful to explain why its use for certain purposes would be legally prohibited, while its use for others—all those not related to law enforcement—would be subject, where appropriate, to a judgement of proportionality.

III. The object of Art. 5

Despite art. 5 AIA being entitled prohibited AI practices, what it really prohibits are certain *actions* in relation to these systems; and generally three actions: 'the placing on the market', 'the putting into service' or 'the use' of AI systems. Placing on the market means 'the first making available of an AI system or a general-purpose AI model on the Union market' (art. 3.9 AIA). Putting into service refers to '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. 3.11 AIA). However, although in general 'placing on the market', 'putting into service', and 'use' of prohibited AI systems are banned, it is important to note that

[12] In this regard, amongst others, Barkane, Questioning the EU proposal for an Artificial Intelligence Act: The need for prohibitions and a stricter approach to biometric surveillance, Information Polity, 2022, 147, 154. It should be noted that, according to recital 45, 'law enforcement authorities' means 'any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security'.

[13] Smuha, N., Ahmed-Rengers, E., Harkens, A., Li, W., MacLaren, J., Piselli, R., Yeung, K., How the Eu can achieve legally trustworthy AI, ob. Cit., pp.25-26.

[14] EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18 de junio de 2021, c.32.

for real-time remote biometric identification systems, only the use is banned, not the other actions, meaning it would be possible to place them on the market and put them into service; although it is not clear why this case is more permissive than the others in art. 5 AIA.

In relation to these actions, it seems clear that placing on the market is *ad intra* in nature as it is confined to the European market. The issue may lie with putting systems into service, given that the supply for first use directly to the deployer ('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 AIA) is not restricted to the European Union—as nothing is specified. In this way it would seem, according to the legal text, that supply of an AI system *ad extra*—outside the Union; in other words, exporting such a system—may be considered to fall within the definition of putting into service and therefore be prohibited generally by art. 5 AIA.

However, this interpretation of the definition is ruled out by the scope of application of the Act laid out in art. 2 AIA. It only applies to those responsible for deploying AI systems *that are established or located in the Union* but not to those in third countries—which is the previous hypothesis. Therefore, the only putting into service that is subject to the Act is *ad intra*, in other words, by those responsible for deployment of AI systems in the Union. And according to art. 2 AIA, those who are subject to the scope of application of the Act include, among others, 'providers placing on the market or putting into service AI systems or placing on the market general-purpose AI models in the Union, irrespective of whether those providers are established or located' [art. 2.1 a) AIA]—to ensure, states recital 21, 'a level playing field and an effective protection of rights and freedoms of individuals across the Union'; 'deployers of AI systems that have their place of establishment or are located within the Union' [art. 2.1 b) AIA]; as well as 'providers and deployers of AI systems that have their place of establishment or are located in a third country, where the output produced by the AI system is used in the Union' [art. 2.1 c) AIA][15].

The Act is therefore applicable to situations that are linked to the Union, whether by the location of the supplier or those responsible for deployment, or by the effects of

[15] According to recital 22, 'this is the case, for example, where an operator established in the Union contracts certain services to an operator established in a third country in relation to an activity to be performed by an AI system that would qualify as high-risk. In those circumstances, the AI system used in a third country by the operator could process data lawfully collected in and transferred from the Union, and provide to the contracting operator in the Union the output of that AI system resulting from that processing, without that AI system being placed on the market, put into service or used in the Union. To prevent the circumvention of this Regulation and to ensure an effective protection of natural persons located in the Union, this Regulation should also apply to providers and deployers of AI systems that are established in a third country, to the extent the output produced by those systems is intended to be used in the Union'.

using AI systems within it[16]. Hence, AI systems suppliers whose business is exclusively with non-Union states are outside of the scope of application, meaning that it is possible for prohibited systems to be sold by European suppliers to third countries[17] (as long as the results of that export are not used in the Union). In fact, as some authors have already noted, the French firm Idemia/Morpho has sold a facial recognition system to the Shanghai Public Security Bureau and likewise, the Dutch firm Noldus has sold a tool for analysing facial expressions (Facereader) to the Chinese Public Security Ministry[18].

Nonetheless, during the legislative process for the text, parliamentarians insisted on the need to prohibit export of AI systems that were prohibited by the Act[19]. The European Parliament attempted to introduce the following amendment regarding recital 20 (old recital 10): 'In order for the Union to be true to its fundamental values, AI systems intended to be used for practices that are considered unacceptable by this Act, should equally be deemed to be unacceptable outside the Union because of their particularly harmful effect to fundamental rights as enshrined in the Charter. Therefore it is appropriate to prohibit the export of such AI systems to third countries by providers residing in the Union' (amendment 29). In line with that, Parliament proposed that the scope of application of the Act (art. 2.1 AIA) should include 'providers placing on the market or putting into service AI systems referred to in Article 5 outside the Union where the provider or distributor of such systems is located within the Union' (amendment 147). Those attempts, however, were rejected after long negotiation[20]. That being the case, the final option of European legislators, while being less of an obstacle to European providers' commercial activities in third countries, would also considerably lessen the 'Brussels effect'[21]. This effect is not, or should not be, projecting *ad extra* a merely formal regulatory model, but rather at its core, material protection of fundamental rights,

[16] Ortega Giménez, El ámbito de aplicación territorial del Reglamento de inteligencia artificial, in Cotino Hueso and Simón (Eds.), Tratado del Reglamento de inteligencia artificial de la Unión Europea, 2024.

[17] López Tarruella Martínez, El futuro reglamento de Inteligencia Artificial y las relaciones con terceros Estados, Revista Electrónica de Estudios Internacionales, 2023, 1, 15.

[18] Veale and Zuiderveen Borgesius, Demystifying the Draft EU Artificial Intelligence Act — Analysing the good, the bad, and the unclear elements of the proposed approach, Computer Law Review International, 2021, 97, 101.

[19] This was also a proposal from Cserne, Ducato, Zivkovic, Brown, Couzigou, Leontidis, Oren, Sutherland, Sweeney, Yuksel Ripley, Commentary to the Commission's proposal for the "AI Act" – Response to selected issues, Centre for Commercial Law, School of Law, University of Aberdeen, 2021, p. 4: https://www.abdn.ac.uk/media/site/law/documents/UoA_CCL_response.pdf

[20] Wachter, Limitations and Loopholes in the EU AI Act and AI Liability Directives: What This Means for the European Union, the United States, and Beyond, Yale Journal of Law & Technology, 2024, 671, 681.

[21] Bradford, The Brussels Effect, Northwestern University Law Review, 2012, 107.

ensuring that Europe does not act as an agent of harm to those rights in the global market—and not just in its own market[22]. It is not for nothing that recital 8 in the AIA underscores that this is about promoting 'the European human-centric approach to AI and being a global leader in the development of secure, trustworthy and ethical AI'. However, the extraterritoriality of the regulation occurs when those affected by AI systems are European citizens, rather than in any other case.

In any event, if prohibited AI systems are put on the market, put into service, or used, the administrative fine prescribed is €35,000, or if the offender is a business, 7% of their worldwide annual turnover in the previous financial year, if that is greater (art. 99.3 AIA). In addition, the European Data Protection Supervisor may impose administrative fines on Union institutions, bodies, and agencies of up to €1,500,000 for failure to comply with the prohibition of AI practices (art. 100.2 AIA).

IV. The prohibitions of Art. 5 are not numerus clausus

Although art. 5 AIA stringently establishes certain prohibited AI practices, not all AI practices are prohibited by the article. The prohibitions therefore go beyond this provision—which is in this regard not a *numerus clausus* system—meaning that a more global or harmonized view of regulation on this matter is needed in order to be able to determine what is, or may be, prohibited.

In the first place, one must bear in mind that art. 5.8 AIA states that the prohibitions laid out by the article do not affect others that may come from AI practices infringing other European Union law. This means that an AI practice may be prohibited despite not being within art. 5 AIA if it contravenes some other law, 'including data protection law, non-discrimination law, consumer protection law, and competition law, should not be affected by this Regulation' (recital 45). Therefore, what is legally prohibited without AI is also prohibited when it is used[23]. This makes it clear that the parameters of legality of AI systems are not solely shaped by the Act, but by the rest of Union law. For example, the well-known Spanish supermarket chain, Mercadona, was recently sanctioned by the AEPD (Spanish Data Protection Agency) for using facial recognition

[22] Noted by Almada and Radu, The Brussels Side-Effect: How the AI Act Can Reduce the Global Reach of EU Policy, German Law Journal, 2024, 646, 657. They explain that in order for the Brussels effect to occur, there must be indivisibility of the object of regulation such that it would not be the case if there were AI systems for the European market and different systems created for other jurisdictions. Although in relation to real-time biometric recognition systems for law enforcement purposes, where the prohibition only refers to use, Díaz González maintains the same, Prohibited Artificial Intelligence Practices (Article 5), ob. cit.

[23] Voigt and Hullen, What AI Practices Are Prohibited?, in P. Voigt and Hullen (Eds.), The EU AI Act. Answers to Frequently Asked Questions, 2024, 1, 38.

in some of its stores to prevent people who had committed offences against its employees or property—and who had been found guilty and bound by restraining orders—from entering the store. Use of such a biometric identification system is prohibited based on art. 9 GDPR, and also contravenes other previsions of that legislation[24]. So although the AIA only prohibits real-time biometric identification systems in publicly accessibly spaces for law enforcement purposes (art. 5.1 h AIA), their use by private subjects may be prohibited—as in this case—based on the GDPR.

Finally, it is important to highlight that the prohibited practices are those currently laid out in art. 5 AIA. This may change over time. Art. 112 AIA tasks the European Commission with an annual evaluation of 'the need for amendment of the list set out in Annex III and of the list of prohibited AI practices laid down in Article 5', meaning a review and revision of what systems are considered prohibited in light of technical progress, presenting their conclusions to the European Parliament and the Council. This provision was included thanks to an amendment from the European Parliament as the initial text from the Commission only considered the possibility of review to modify the list in Appendix III (high-risk systems).

This seems clearly necessary given that the regulations are about an area of knowledge that changes extremely rapidly, meaning that periodic review is essential to avoid it becoming obsolete and leading to harm to health, security, and fundamental rights[25]. These are all aspects that, along with advances in the information society, the Commission should take into account when formulating their proposed revisions (art. 112.10 AIA). Hence, practices not prohibited now may become so in the future, perhaps because they do not exist currently, or maybe because their potential harm is unknown or cannot be shown (this is always easier to do once they are put into practice). The opposite may also occur; currently prohibited practices may become permitted if technical progress allows them to be implemented without contravening people's fundamental rights.

While there is a need to avoid regulatory obsolescence weakening protection of people's fundamental rights, security, and health, perhaps it would have been more satisfactory had there been a process allowing the Commission itself to alter the list of AI practices prohibited by art. 5 AIA in concert with other actors. This would have been possible had the Commission been allowed to adopt delegated acts in relation to art. 5 AIA—in the same way it is allowed to modify Appendix II by adding or modifying high-risk AI systems (art. 7 and 97 AIA)—to avoid having to fall back on the ordinary

[24] Proceeding No: PS/00120/2021. May be found at: https://www.aepd.es/documento/ps-00120-2021.pdf.

[25] Legal scholarship has already highlighted this need. See, for example, Smuha, N., Ahmed-Rengers, E., Harkens, A., Li, W., MacLaren, J., Piselli, R., Yeung, K., How the EU can achieve legally trustworthy AI, ob. Cit, pp.221.

legislative process, the lengthy nature of which might provide cover for diminishing legal protection[26].

Lastly, it is important to mention that permitted AI practices (as such, outside the scope of art. 5 AIA) may not be usable if they do not comply with the specific obligations laid out in the Act. Consider, for example, high-risk systems that do not pass conformity assessments (art. 43 AIA). Although the effects may be the same in practical terms—not being able to use the systems—these are clearly very different situations than those in art. 5 AIA. There are some AI systems that by their very nature or purposes/effects are contrary to fundamental rights and values of the European Union, and others that are compatible in principle but cannot be used if they do not comply with certain regulations imposed by the Act. In this latter case, permission to use is related to the guarantees and controls established in the Act meaning that nonconformity could be addressed if these are observed, something that does not happen in the case of art. 5 AIA. In any case, this point serves to illustrate that art. 5 AIA is not the sole method of preventing AI systems from being placed on the market, put into service, or used.

V. Absolute prohibitions vs. Relative prohibitions

Although art. 5 AIA lays out all of the prohibited AI practices, it is important to emphasize that not all of the prohibitions are the same. In some cases—perhaps the minority—the *prohibitions are absolute* in the sense that they prohibit certain systems *per se*, without the ban being affected by the system having certain effects or results. This is the case, for example, of systems for making risk assessments of natural persons, facial recognition databases, emotion recognition systems, and biometric categorization systems. The systems in these cases are prohibited without considering additional variables related to their use or implementation.

In other situations, however, art. 5 AIA sets out what we might call *relative* or *conditional prohibitions* in the sense that they exclude certain AI systems but only in that they produce certain effects or consequences, or have certain specific objectives[27]. This means that the same system may be prohibited or not based on the consequences of its use. This is what happens, firstly, with AI systems that use subliminal, manipulative, or deceptive techniques, which are prohibited if they do so 'with the objective, or the effect of materially distorting the behaviour of a person or a group of persons' [art. 5.1 a)

[26] This was the proposal from Smuha, N., Ahmed-Rengers, E., Harkens, A., Li, W., MacLaren, J., Piselli, R., Yeung, K., How the Eu can achieve legally trustworthy AI, ob. Cit p.21; seconded by (among others) Díaz González, Prohibited Artificial Intelligence Practices (Article 5), ob. cit.

[27] This issue was already highlighted by, among others, Miguez Macho and Torres Carlos, Sistemas de IA prohibidos y sistemas de IA de alto riesgo, in Barrio Andrés, M. et al. (Eds.), El Reglamento Europeo de Inteligencia Artificial, 2024, p.55.

AIA]. The same applies to AI systems that exploit a person or group's vulnerabilities, which are only prohibited if they have this 'objective or effect' [art. 5.1 b) AIA]. It is not necessary, therefore, for them to be used with the intention of altering subjects' behaviours, something which seems to be covered by the terms 'objective' and 'purpose', which indicate a volitional component, and was requested in the original Commission proposal[28]. It is sufficient that this situation is produced, in other words, that the AI system merely produces this 'effect'[29]. The important issue here is that without that purpose or effect, the prohibitions do not operate.

What can happen, however, is that these conditions may be (and in many cases are) cumulative, meaning that a chain of them is needed to trigger the prohibition. In the case of manipulative AI techniques, there is the additional requirement of affecting people, 'causing them to take a decision that they would not have otherwise taken', and that this 'causes or is reasonably likely to cause that person, another person or group of persons significant harm'. For AI systems that exploit vulnerabilities, only the latter condition is laid out. So there is a cumulative requirement of two or three effects: substantial change in behaviour, taking a decision that they otherwise would not have taken (only in the case of manipulative techniques), and causing or being reasonably likely to cause significant harm. A prohibition would only be put into place if all of these conditions were met.

Secondly, another example of relative prohibition may be found in social scoring systems, because, along with the other elements required by [art. 5.1 c) AIA], such systems are only prohibited if the resultant social scoring system causes a certain result: 'detrimental or unfavourable treatment of certain natural persons or groups of persons in social contexts that are unrelated to the contexts in which the data was originally generated or collected'; and/or 'detrimental or unfavourable treatment of certain natural persons or groups of persons that is unjustified or disproportionate to their social behaviour or its gravity'. This means that social scoring systems that classify people based on their behaviour or personal characteristics are not in and of themselves prohibited, but only when they cause this detrimental or unfavourable treatment. They would, for example, be permitted for classifying a worker using data related to a given

[28] Art. 5.1 a) RIA, in the Commission proposal, state: 'the placing on the market, putting into service or use of an AI system that deploys subliminal techniques beyond a person's consciousness in order to materially distort a person's behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm'. This is highlighted by, for example, Veale and Zuiderveen Borgesius, Demystifying the Draft EU Artificial Intelligence Act — Analysing the good, the bad, and the unclear elements of the proposed approach, ob. Cit. p.99; Nikolinakos, N.T., EU Policy and Legal Framework for Artificial Intelligence, Robotics and Related Technologies - The AI Act, 2023, pp.376-377.

[29] Fernández Hernández, C., Capítulo II. Prácticas de IA Prohibidas, in Barrio Andrés (Ed.), Comentarios al Reglamento Europeo de Inteligencia Artificial, 2024.

employment relationship (the same context) as long as they do not cause disproportionate unfavourable treatment.

Lastly, real-time remote biometric identification systems [art. 5.1h) AIA] would also be subject—according to this argument—to relative prohibitions. And unlike the previous cases, what is applied according to the conditions is the exception to the prohibition. In other words, such systems are prohibited 'unless and in so far as such use is strictly necessary for one of the following objectives', which are set down in the clauses of art. 5.1 h) AIA. So this means that real-time remote biometric identification systems are prohibited *if they are not in pursuit* of one of the legally established objectives. The prohibition is affected in any case, albeit negatively.

The conditional or relative prohibitions make it easier to see the risk-based focus that runs through the Act. There are some practices that are prohibited because the unacceptable risks to the Union's fundamental rights and values are only seen if certain effects/purposes occur—which increase the risks exponentially—otherwise they are not. This may only be assessed on a case by case basis. To put it another way, this shows a 'graduated' legal response—accompanying the risk—that is not apparent in absolute prohibitions (by their very nature), which only offer a single response to what may be a range of variables in one practice.

Establishing these conditional types of prohibition poses added difficulties. Firstly, it gives a wide margin of discretion to the bodies that apply the Act. They may, among other things, feel obliged to perform some kind of *judgement of reasonability or suitability* to substantiate the link between the specific AI practice and the corresponding consequences the Act lays out (effect, harm, etc.) of its use, putting into service, or introducing into the market. However, the main difficulty would be in determining the concurrency of the conditions when in many cases they are not events or circumstances that have happened (*ex post* conditions). In many cases they may be intentions—that the AI system is used with a certain 'purpose' or 'objective'. In other cases they may be possibilities or risks (*ex ante* elements), for example causing 'or being reasonably likely to cause' harm, etc. The concurrence of such elements—without a factual basis—is much harder to confirm, necessitating preventive or probabilistic judgements, which seem to be prone to greater levels of interpretability.

VI. The limited scope of Art. 5 AIA

Despite art. 5 AIA covering a broad catalogue of prohibited practices, as we have emphasized above, it is in fact less restrictive than it might seem at first glance. In the first place, its limited scope is because the prohibitions have a scope of application which is generally relatively narrow. On the whole, various elements need to occur together cumulatively for the prohibitions to be activated. These are sometimes consequences or

effects produced by the AI systems. However, many other times they are objective elements, such as the system having certain characteristics or operating in certain contexts. This clearly makes practical application of such cases more difficult because it needs the successive concurrence of various factors which in some cases are not easy to prove. If only one of them is absent or unproven, the prohibition will not be applicable.

For example, art. 5 AIA does not make a general prohibition of predictive policing systems for individuals. It prohibits (1) an 'AI system for making risk assessments of natural persons'—which excludes systems assessing crime risk by area or locations; (2) 'in order to assess or predict the risk of a natural person committing a criminal offence'—which excludes the use of these mechanisms for investigating an existing offence (*ex post*), i.e., for investigative purposes, as well as excluding administrative infractions; (3) 'based solely on the profiling of a natural person or on assessing their personality traits and characteristics'—which permits the use of AI systems based on other factors (although the above also apply), such as systems that use 'risk analytics to assess the likelihood of financial fraud by undertakings on the basis of suspicious transactions or risk analytic tools to predict the likelihood of the localisation of narcotics or illicit goods by customs authorities, for example on the basis of known trafficking routes' (recital 42).

Secondly, art. 5 AIA has many exceptions to the different prohibition cases. See, for example, the exception for 'AI systems used to support the human assessment of the involvement of a person in a criminal activity, which is already based on objective and verifiable facts directly linked to a criminal activity', which is set out as an exception for individual predictive policing systems[art. 5.1 d)A]; emotion recognition systems in the workplace and education 'intended to be put in place or into the market for medical or safety reasons' [art. 5.1 f) RIA] 'such as systems intended for therapeutical use' (recital 44); and the exclusion of 'labelling or filtering of lawfully acquired biometric datasets, such as images, based on biometric data or categorizing of biometric data in the area of law enforcement' [art. 5.1 g) RIA].

These exceptions are supplemented by those for real-time remote biometric identification systems in public spaces for law enforcement purposes, which are allowed when necessary for certain objectives laid out in art. 5.1 h) RIA: 'the targeted search for specific victims of abduction, trafficking in human beings or sexual exploitation of human beings, as well as the search for missing persons'; 'the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or a genuine and present or genuine and foreseeable threat of a terrorist attack'; and 'the localisation or identification of a person suspected of having committed a criminal offence, for the purpose of conducting a criminal investigation or prosecution or executing a criminal penalty for offences referred to in Annex II and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least

four years'. In fact, rather than a prohibition, this seems like a detailed regulation of the guarantees such systems must have when they are used for these specific purposes[30], which is in effect what the extended text of art.5 AIA is largely concerned with.

The problem of exceptions is not that they exist, but rather that, as clauses that operate as limitations to subjects' fundamental rights, they must be properly justified: they should be necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others (art. 52 CFREU). In addition, exceptions should be worded a certain, precise way to satisfy the exigence of being provided by law (art. 52 CFREU). This also avoids ambiguity or overbroad wording which might make an exception into a useful way to circumvent a prohibition. Vagueness of prohibitions may, in short, undermine the rights-based purpose of art. 5 and hence harm the fundamental rights of those involved. For example, in relation to individual police predictive support systems, set out as an exception, it is not clear what level of human intervention is needed for such a system to be permitted. Is one person enough? What must they be doing? This is problematic, additionally bearing in mind automation bias that may reduce human intervention to a mere formality. Something similar may occur for medical, and particularly security reasons, which may support the use of emotion recognition systems in the workplace and in education, as they may be interpreted with different scope, by different actors, in such contexts[31].

Thirdly, it is important to bear in mind that, when defining the scope of application, art. 2 AIA excludes certain cases. Art. 2.3 AIA is particularly important here, stating that it will not apply to AI systems 'where and in so far they are placed on the market, put into service, or used with or without modification exclusively for military, defence or national security purposes, regardless of the type of entity carrying out those activities' (art. 2.3 AIA), in other words public or private. Nor will it apply to AI systems which are not placed on the market or put into service in the Union, where the output is used in the Union exclusively for military, defence or national security purposes, regardless of the type of entity carrying out those activities. The original proposal from the Commission, however, only contained the exclusion for military purposes, not the other two (defence and national security), which were proposed by the Council and ultimately included. This exclusion—referring to national security and defence—was

[30] This was noted by, among others, Smuha, N., Ahmed-Rengers, E., Harkens, A., Li, W., MacLaren, J., Piselli, R., Yeung, K., How the Eu can achieve legally trustworthy AI, ob. Cit, p.26. The limited scope of the prohibition was also noted by Barkane, Questioning the EU proposal for an Artificial Intelligence Act: The need for prohibitions and a stricter approach to biometric surveillance,, ob. Cit., p.153.

[31] Cemalovic, Prohibited Artificial Intelligence Practices according to art. 5 of the European Union's regulation on AI – between the too late and the not enough, International Journal of Law and Information Technology, 2024, 1, 11.

also included in the Framework Convention on Artificial Intelligence (art. 3.2 and 3.4)[32].

Therefore, these prohibited AI practices, if they are used exclusively with these purposes, must end up being permitted. However, where the same systems are used for other purposes as well (law enforcement, public safety, etc.)—so called 'dual-use systems'—then they are subject to the Act. The exception only operates for systems that are introduced onto the market, put into service, or used *exclusively* for the purposes noted above. That exclusivity breaks when initially excluded systems are used temporarily or permanently for other purposes or when such uses occur at the same time, being introduced into the market, put into service, or used for an excluded purpose and for one or more non-excluded purposes.

According to recital 24, this exclusion in relation to military or defence purposes 'is justified both by Article 4(2) TEU and by the specificities of the Member States' and the common Union defence policy covered by Chapter 2 of Title V TEU that are subject to public international law, which is therefore the more appropriate legal framework for the regulation of AI systems in the context of the use of lethal force and other AI systems in the context of military and defence activities. As regards national security purposes, the exclusion is justified both by the fact that national security remains the sole responsibility of Member States in accordance with Article 4(2) TEU and by the specific nature and operational needs of national security activities and specific national rules applicable to those activities'. Nonetheless, art.2.3 AIA specifies that the Act will not affect the competencies of member states in matters of national security, 'regardless of the type of entity entrusted by the Member States with carrying out tasks in relation to those competences'. This means that prohibited AI practices may also be implemented by private actors on behalf of member states who have outsourced national security tasks to them[33]. Although the CJEU has defined what national security is[34], it has been argued that the interpretation of the—already very broad—concept may vary from state to state, and may also be easily confused with public safety (whose activities are subject to the Act), making legal certainty difficult in relation to the scope of application of the exception.

---

[32] For a legal comparison of the two texts, see the work of Presno Linera and Meuwese, La regulación europea de la Inteligencia Artificial, Teoría y Realidad Constitucional, 2024, 131.

[33] Gómez de Ágreda, La exclusión de los sistemas inteligencia artificial de seguridad nacional, defensa y militares del Reglamento y el Derecho aplicable, in Cotino Hueso and Simón (Eds.), Tratado del Reglamento de inteligencia artificial de la Unión Europea, Aranzadi-La Ley, 2024.

[34] It relates 'to the primary interest in protecting the essential functions of the State and the fundamental interests of society and encompasses the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities' (CJEU, C-511/18, La Quadrature du Net and Others v Premier ministre and Others, ECLI:EU:C:2020:791, para 135)

In this regard, art. 2.3 AIA seems to constitute the first—and very large—exception to art. 5 AIA. It is not, therefore, unreasonable to think that the invocation of national security—with the legal problems of interpretation noted above—might serve as a pretext for resorting to using prohibited practices based on a need to safeguard it. Consider, for example, the use of some of these prohibited systems for border control, or others such as general predictive policing systems, which may be more susceptible to being used under such a cover.

However, it is worth bearing in mind that use of potential prohibited AI systems under the protection of art. 2.3 AIA will not take place in a legal vacuum. The CJEU has indicated that 'although it is for the Member States to define their essential security interests and to adopt appropriate measures to ensure their internal and external security, the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with that law'. Therefore, in so far as the pursuit of these purposes involves using AI systems that need, for example, data processing activity that involve entities subject to Union law—such as data being collected by private actors—, then such AI systems, despite falling under the art. 2.3 AIA exception, will be subject to, among other things, European data protection legislation and the EU Charter of Fundamental Rights[35].

Finally, it is also important to emphasise that the less than restrictive scope of art. 5 AIA is because, in certain cases, AI systems that it would prohibit are already prohibited by other provisions in Union law. These provisions are in primary legislation such as, but not exclusive to, the EU Charter of Fundamental Rights, the General Data Protection Act, (EU) Directive 2016/680, and in the European Convention on Human Rights. For example, without being exhaustive, biometric categorization systems used to 'infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation' may be considered to already by covered by the prohibition in art. 9.1 GDPR, which prohibits treatment of personal data 'revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation'. Alternatively, a social rating system that discriminates against a certain group (women, immigrants, etc.) may be prohibited outside of the AIA based on, among other things, art. 14 ECHR and art. 21 CFREU. That is not to say, obviously, that art. 5 AIA is not needed, but rather that perhaps it has created *ex novo* fewer prohibitions in the Union than an initial reading might have suggested.

[35] Korff, Opinion on the implications of the exclusion from new binding European instruments on the use of AI in military, national security and transnational law enforcement contexts, European Center for Not-for-Profit Law, 2022, https://ecnl.org/sites/default/files/202210/ECNL%20Opinion%20AI%20national%20security_0.pdf.

VII. Brief conclusions

Art. 5 AIA aims to resolve the difficult balancing act between the protection of the European Union's fundamental rights and values, and the promotion of technological progress within the Union and around the world. The finally approved text, in contrast to the Commission's original proposal, is more restrictive as it is often broader in the proposed prohibitions' objective and subjective scope, also allowing annual review to prevent legislative obsolescence from weakening the protection of the fundamental rights at stake. It is also the result of a particularly participative process, involving not only European institutional actors, but other non-legislative bodies who, in various ways, attempted to put forward their own proposals, many of which—as we have seen—were ultimately accepted.

Nonetheless, despite the Act's laudable intentions, it does have some weaknesses that may contribute to weakening its attempts at protecting fundamental rights. Despite an undeniably restrictive appearance, the reality is, in practice, less so. Firstly, some of the prohibitions the Act establishes are already covered by different Union legislation, meaning that in some cases, it does not add any additional limitations. What is not allowed without AI is not allowed with AI. Secondly, because export of prohibited AI practices to countries outside the EU is permitted, this considerably reduces the Brussels effect of protecting fundamental rights on a global level. Thirdly, many of the prohibitions either have many exceptions to their application or have cumulative requirements—some of which are very difficult to monitor—that need to exist concurrently for the prohibitions to apply. This concurrency will often be difficult to prove. And this is without forgetting that fact that in general, art.5 AIA is occasionally worded very broadly or in very abstract terms, making it hard to determine what it really covers. This issue will not only need the interpretive efforts of the Commission—who are called on to publish directives on the practical application of art. 5 AIA (art. 96.1b AIA)—but also the bodies that apply the law. Applying the regulation to specific cases will help to more precisely outline its scope of application.

VIII. References

Almada and Radu, The Brussels Side-Effect: How the AI Act Can Reduce the Global Reach of EU Policy, German Law Journal, 2024, 646.

Barkane, Questioning the EU proposal for an Artificial Intelligence Act: The need for prohibitions and a stricter approach to biometric surveillance*, Information Polity*, 2022, 147.

Bradford, The Brussels Effect, Northwestern University Law Review, 2012, 107.

Carlon, Las Administraciones Públicas ante la Inteligencia Artificial, 2025.

Cemalovic, Prohibited Artificial Intelligence Practices according to art.5 of the European Union's regulation on AI – between the too late and the not enough, International Journal of Law and Information Technology, 2024, 1.

Cserne, Ducato, Zivkovic, Brown, Couzigou, Leontidis, Oren, Sutherland, Sweeney, Yuksel Ripley, Commentary to the Commission's proposal for the "AI Act" – Response to selected issues, Centre for Commercial Law, School of Law, University of Aberdeen, 2021, https://www.abdn.ac.uk/media/site/law/documents/UoA_CCL_response.pdf

De Gregorio and Dunn, The European risk-based approaches: Connecting constitutional dots in the digital age, Common Market Law Review, 2022, 473

Díaz González, Prohibited Artificial Intelligence Practices (Article 5), in Huergo Lora and Díaz González (Eds.), The EU Regulation on Arificial Intelligence: A Commentary, 2025 (forthcoming).

Fernández Hernández, C., Capítulo II. Prácticas de IA Prohibidas, in Barrio Andrés (Ed.), Comentarios al Reglamento Europeo de Inteligencia Artificial, 2024

López Tarruella Martínez, El futuro reglamento de Inteligencia Artificial y las relaciones con terceros Estados, Revista Electrónica de Estudios Internacionales, 2023, 1, 15.

Gómez de Ágreda, La exclusión de los sistemas inteligencia artificial de seguridad nacional, defensa y militares del Reglamento y el Derecho aplicable, in Cotino Hueso and Simón (Eds.), Tratado del Reglamento de inteligencia artificial de la Unión Europea, Aranzadi-La Ley, 2024.

Korff, Opinion on the implications of the exclusion from new binding European instruments on the use of AI in military, national security and transnational law enforcement contexts, European Center for Not-for-Profit Law, 2022. https://ecnl.org/sites/default/files/202210/ECNL%20Opinion%20AI%20national%20security_0.pdf

Miguez Macho and Torres Carlos, Sistemas de IA prohibidos y sistemas de IA de alto riesgo, in Barrio Andrés, M. et al. (Eds.), El Reglamento Europeo de Inteligencia Artificial, 2024, 48.

Nikolinakos, EU Policy and Legal Framework for Artificial Intelligence, Robotics and Related Technologies - The AI Act, 2023.

Ortega Giménez, El ámbito de aplicación territorial del Reglamento de inteligencia artificial, in Cotino Hueso and Simón (Eds.), Tratado del Reglamento de inteligencia artificial de la Unión Europea, 2024.

Presno Linera, La propuesta de Ley de Inteligencia Artificial Europea, Revista de las Cortes Generales, 2023, 81.

Presno Linera and Meuwese, La regulación europea de la Inteligencia Artificial, Teoría y Realidad Constitucional, 2024, 131.

Smuha, N., Ahmed-Rengers, E., Harkens, A., Li, W., MacLaren, J., Piselli, R., Yeung, K., *How the Eu can achieve legally trustworthy AI*, LEADS Lab University of Birmingham, 2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3899991

Wachter, Limitations and Loopholes in the EU AI Act and AI Liability Directives: What This Means for the European Union, the United States, and Beyond, Yale Journal of Law & Technology, 2024, 671.

Veale and Zuiderveen Borgesius, Demystifying the Draft EU Artificial Intelligence Act — Analysing the good, the bad, and the unclear elements of the proposed approach, Computer Law Review International, 2021, 97

Voigt and Hullen, What AI Practices Are Prohibited?, in P. Voigt and Hullen (Eds.), The EU AI Act. Answers to Frequently Asked Questions, 2024.