European AI Regulation: Brussels Effect versus Human Dignity?

Oskar J. Gstrein*

Table of Contents

Abstract

The European Commission proposal for a legal framework to comprehensively regulate Artificial Intelligence (AI) came after years of public consultation and deliberation. Most prominently the AI High Level Expert Group (AI HLEG) prepared ethical guidelines and policy recommendations since 2018. While countries such as China and the United States, or international organisations such as the Council of Europe work on legal frameworks to regulate the development and use of AI, the European Commission's proposal (AI Act or AIA) presented on 21 April 2021 seems to put the Union in the most powerful position to establish regulatory standards with global relevance for a key emerging technology. After shortly summarising the origin, context and main characteristics of the prospective regulation, this article explores whether the 'Brussels Effect' will manifest in ground-breaking AI regulation, or whether the Union and its Member States run the risk of hastily adopting an incapable legal framework for a technology whose effects on society are still insufficiently understood. Furthermore, it remains open whether the proposed

* Programme Director BSc Data Science and Society, Assist. Prof. Governance and Innovation, Member Data Research Centre, Campus Fryslân – University of Groningen (Netherlands), NL. Email: oj@gstrein.info. This article has benefitted from the discussions around the event "Malicious (ab)use of Artificial Intelligence", held on 29 August 2022 at the Humboldt Institute for Internet and Society (HIIG) in Berlin, Germany. A particular thanks goes to Taís F. Blauth for organising the event and Andrej Zwitter.

AIA integrates with existing and emerging legal frameworks, potentially watering down the commitment of the EU to protect human rights and human dignity.

Keywords: Artificial Intelligence, Regulation, AI Act, AIA, Brussels Effect, Human Dignity, Human Rights, Governance, Datafication

A. Introduction

The control of emerging technologies such as Artificial Intelligence (AI) is a strategic priority for political leaders all over the world. The knowledge and control around the development and deployment of AI is important from a military and security perspective.[1] Economically exploitable AI capabilities hold many promises as it seems to become a general-purpose technology facilitating prediction and decision-making in particular.[2] However, with the broad societal adoption and deployment of AI-infused technologies and systems an increasing number of potential risks, harms, and threats have been mapped by academics and civil society organisations.[3] As impressive as the technological and economic potential of the further development and adoption of AI in all of its imaginable forms seem, as urgent become the risks and challenges in developing and deploying AI in a way that promotes human dignity and broad social welfare by default. In recent years this tension sparked a continuing discussion around the ethically and politically desirable use of AI,[4] which more recently turned to developing legally binding frameworks.

In the European Union (EU) this process manifested through the creation of an expert group with members from different societal stakeholder groups, starting on 9 March 2018.[5] To date this group has produced four deliverables including ethical guidelines for trustworthy AI,[6] an assessment list for trustworthy AI, policy and investment recommendations for the EU, as well as sectoral considerations for these recommendations. While these documents and accompanying policy initiatives con-

1 *Haner/Garcia*, Global Policy Volume 2019/10, p. 331–337; *Blauth/Gstrein/Zwitter,* IEEE Access 2022, p. 77110–77111.

2 *OECD*, Artificial Intelligence in Society 2019, p. 35–46.

3 *Chiusi* et al., Automating Society Report 2020, available at: https://automatingsociety.algorithmwatch.org/wp-content/uploads/2020/12/Automating-Society-Report-2020.pdf (18/10/2022); *Mozilla Foundation*, Internet Health Report 2022 – AI in Real Life, available at: https://2022.internethealthreport.org/ (18/10/2022); *Crawford*, p. 211–229.

4 See e.g. *Nemitz*, Phil.Trans.R.Soc. 2018, p. 2–13; *Hildebrandt*, Phil.Trans.R.Soc. 2018, p. 2–9.

5 *European Commission*, Artificial intelligence: Commission kicks off work on marrying cutting-edge technology and ethical standards, available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_18_1381 (18/10/2022).

6 In the public perception this was probably the most influential deliverable to date. The guidelines promote a 'human-centric approach' on AI and suggest seven key requirements: human agency and oversight, technical robustness and safety, privacy and data governance, transparency, diversity as well as non-discrimination and fairness, societal and environmental well-being, and accountability. The full guidelines are available at: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419 (18/10/2022).

tinue to be influential in debates around discrimination due to reenforced historic biases in automated decision-making systems,[7] a lack of explainability of automated decisions,[8] badly designed AI systems due to oversimplification of complex societal problems,[9] as well as the use of insufficient and unrepresentative training data sets to train algorithms,[10] the discourse around AI in the EU has recently pivoted towards considering legally binding rules. On 21 April 2021 the European Commission tabled a draft for a comprehensive legal framework governing the development and use of AI in many application scenarios.[11]

This Commission Proposal for a Regulation "Laying Down Harmonised Rules on AI" (AI Act or AIA hereafter) has surprised many observers and experts. Since the protection of privacy and personal data have become a fundamental rights issue starting in the early 2000s,[12] ultimately catalysing the creation of the highly influential 2016 General Data Protection Regulation (GDPR),[13] many expected the Commission to propose a similar human-rights-focused strategy for AI regulation. But despite the rich ethical discussion and human rights basis of EU law, the Commission proposal is heavily focused on standardisation and harmonisation of the single market. Certainly, the proposal still mentions Article 16 TFEU—a provision relating to the protection of personal data which is also central to GDPR—as legal basis in the Union's founding treaties. However, when looking closer at the subject matter in Art. 1 of the draft AIA, it becomes clear that harmonisation and standardisation based on Art. 114 TFEU—a famous provision in EU law allowing for the approximation of laws for the single market through a co-decision procedure of the European Parliament and the governments of Member States—are the focus of this legal framework. Potentially, there might be some blanket prohibitions of "certain artificial intelligence practices" as mentioned in Art. 1(a) of the draft AIA, but the emphasis is clearly on harmonisation, risk management and transparency.

This leads to the central question of this article: Has the EU chosen an approach for AI regulation that emphasises standard setting and political influence leveraging the 'Brussels Effect', therefore de-prioritising the protection and promotion of human dignity and human rights? This question will be explored by briefly considering the origin and context of the initiative to regulate AI, as well as the main objectives and characteristics of the draft AIA. It is also important to consider how the AIA integrates with existing legal frameworks and similar initiatives, the positioning of the AIA within the Union, as well as speculation on the global positioning of

7 *Crawford*, p. 128–149.
8 *Olsen* et al., in: Hans W. et al. (eds.), p. 219–235; *Gstrein/Zwitter*, Bestuurskunde, p. 30–42.
9 See e.g. *Gstrein/Bunnik/Zwitter*, Católica Law Review 2019/3, p. 77–98.
10 *Angwin* et al., Machine Bias, 23/5/2016, available at: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing (18/10/2022).
11 *European Commission,* Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM(2021) 206 final.
12 *González Fuster*, p. 213–252.
13 *Greenleaf*, Privacy Laws & Business International Report 2022, p. 3–8.

the EU through the new regulation. The objective of this article is to contribute to the growing body of academic literature that attempts to gauge the effects and societal impact of the discussions around the AIA. It attempts to concisely summarise the current situation and to give an outlook for a process that takes place at enormous pace with complex parallel negotiations in the European Parliament and the Council of the EU as main legislators.

In conclusion, by drawing on existing literature discussing the proposal and political developments, it is argued that it is unlikely that the AIA will become a flawless legal framework. It will probably also not become as influential as standard-setting regulatory framework for AI as the GDPR has become for data protection. However, since under current circumstances the EU is the only politically and economically sufficiently influential actor that is willing and capable to regulate the area comprehensively, with a constitutional system clearly referencing human rights, democracy, and the rule of law—therefore, arguably also aiming for a safe and trustworthy use of AI—the AIA will probably become a globally relevant point of departure for the design and deployment of AI for years to come.

B. Origin and Context

Loosely inspired by the dream of "thinking machines" and cybernetic ideology—an approach to understanding processes entirely through observation of information and signals—the term AI was coined during a ten-day workshop in 1956 at Dartmouth College in the United States (US).[14] The prospect of super-intelligent autonomous systems was very appealing in times of the Cold War, and therefore received generous funding from the military sector from the start. Nevertheless, over the following decades of the 20th century the interest in AI was mixed.[15] Furthermore, a precise definition of what constitutes AI is subject to vivid discussion—even dispute—until today.[16] Accordingly, the options for approaches to governance and regulation vary from focusing on "algorithmic regulation",[17] to sectoral approaches for specific (business) contexts, or principle-based approaches that resemble data protection regulation, to name just a few.

At the beginning of the 21st century, the fate of AI and its proponents was decided through the "datafication of society", i.e. seemingly capturing all aspects of societal interaction via digital traces.[18] It is particularly Big Tech companies that increas-

14 *Taulli*, p. 1–11; *Crawford*, p. 1–9.
15 *Taulli*, p. 8–15; *Dean,* Daedalus 2022/151, p. 58.
16 *Larsson/Heintz*, Internet Policy Review 2020/2, p. 2. The draft AIA uses an extremely broad definition for AI systems, which is outlined in Art. 3(1) as "software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with". Since this definition is subject to what is stated in an Annex to that actual regulation, it can also be changed and adapted quite flexibly.
17 *Borges Fortes/Barquero/Restrepo Amariles*, EJRR 2022, p. 3–9.
18 *Gstrein/Beaulieu*, Philos. Technol. 2022/3, p. 5–10.

ingly deploy AI-infused systems to offer novel products and services, as well as powerful nations such as the US and the People's Republic of China (PRC) in a race towards strategic dominance. At the end of a "golden decade for AI" however,[19] many regions of the world are increasingly concerned about the emerging power imbalance in the private and public sphere.[20] Additionally, there is criticism of a "technological solutionism" approach used to tackle any multi-faceted societal problem,[21] such as the COVID-19 pandemic.[22] Finally, an increasing number of reports of harms and risks of using AI systems to make meaningful predictions and decisions fuel the desire for a serious discussion around specific AI regulation.[23]

The EU faces these developments from a dual perspective. First, the bloc considers itself as frontrunner in the regulation of digital technologies. Most prominently this has crystallised in the development and widespread adoption of the GDPR and its principles, which has considerable extraterritorial effect. On the one hand, this extraterritorial effect manifests in the authority that the "European style" of data protection has gained as of 2022; 157 countries in the world do have national data protection laws, most of them following the European—principle-based, technology neutral, covering all sectors of use—omnibus approach. Not only countries drafting novel legal frameworks use the GDPR as model, but also countries revising existing ones.[24] On the other hand, there are provisions with direct extraterritorial effect, such as Art. 3 GDPR covering territorial scope and the regime around adequacy decisions to enable/block international data flows.[25] Furthermore, the GDPR itself contains provisions that relate to the use of AI broadly speaking, most prominently a provision on the use of automated-decision making in a profiling context in Art. 22 GDPR.[26] Building on the GDPR success, more recently additional legal frameworks have been proposed, and partially already adopted. This includes the Union's Digital Services Act (DSA) and Digital Markets Act (DMA),[27] for which it goes beyond the scope of this article to cover them in detail. It is sufficient to state that they should aid equally in reigning in the power of big platforms and technology companies while protecting user rights. Important is however, that the discussion around the AIA must be considered in this context of constantly emerging legislative initiatives responding to various calls from different societal stakeholders.

19 *Dean,* Daedalus 2022/151, p. 69.
20 *Taylor*, in: Gstrein/Zwitter (eds.), p. 9–10.
21 *Morozov,* p. 1–17.
22 See e.g. *Milan,* Big Data & Society 2020, p. 1–7. *Gstrein/Kochenov/Zwitter*, A Terrible Great Idea? COVID-19 'Vaccination Passports' in the Spotlight, available at: https://www.compas.ox.ac.uk/2021/a-terrible-great-idea-covid-19-vaccination-passports-in-the-spotlight/ (18/10/2022).
23 See e.g. *Kilpatrick/Jones*, A clear and present danger Missing safeguards on migration and asylum in the EU's AI Act, available at: https://www.statewatch.org/media/3285/sw-a-clear-and-present-danger-ai-act-migration-11-5-22.pdf (18/10/2022).
24 *Greenleaf,* Privacy Laws & Business International Report 2022, p. 3–8.
25 *Gstrein/Zwitter,* Internet Policy Review 2021/3, p. 7–13.
26 *Bygrave*, in: Kuner/Bygrave/Docksey (eds.), Art. 22 GDPR, p. 526–527.
27 *Burggraf/Gerlach/Wiesner*, Media Perspektiven 2021/5, p. 292–300.

Here mainly, the EU as legislator tries to establish respect, protection and promotion for its values and citizen's interests through regulation of digital technologies.

Secondly, there is an economic incentive to regulating AI, and to do so quickly. The EU and its Member States face economic dependencies when it comes to access and development of emerging technologies and want to make sure that EU countries are significant stakeholders in this area, due to the strategic importance of the technology.[28] The AIA draft proposal clearly mentions these economic objectives when aiming at "ensuring legal certainty to facilitate investment and innovation in AI", wanting to "facilitate the development of a single market", as well as preventing fragmentation of the single market.[29] This ambition to create an innovative and competitive environment can also be seen in the attempt to establish "regulatory sandboxes" (Art. 53-55 draft AIA) that allow for the deployment of innovation and even risky uses of AI in a controlled way.[30]

Certainly, the EU will hope that the "Brussels Effect" once more manifests. This concept has been coined by the scholar Anu Bradford and describes "Europe's unilateral power to regulate global markets."[31] Her argument is that a political actor able to combine five factors including market size, regulatory capacity, stringent standards (e.g. consistent approach to data protection), inelastic targets (e.g. non-mobile consumers), and non-divisibility (e.g. mass-production cost advantage for manufacturers and service providers) is able to determine global regulatory standards for an area such as AI. The effect results from the fact that most globally active corporations adopt the European requirements for designing their products and services, even when it is more costly than when comparing European standards to those in force elsewhere. Since compliance with the EU model enables producers to operate and refine only one product, it can be marketed at scale globally. The EU has been able to establish the Brussels Effect since the 1990s and has become the "global regulatory hegemon" in many areas, according to the theory.[32]

C. Objectives and Main Characteristics of the AIA

In order to reconcile the desire for economic development and high standards for AI safety—ultimately promoting human dignity—the AIA draft proposal contains four specific objectives, namely to:

28 "The way we approach Artificial Intelligence (AI) will define the world we live in the future. To help building a resilient Europe for the Digital Decade, people and businesses should be able to enjoy the benefits of AI while feeling safe and protected." Available at: https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence (18/10/2022).

29 *European Commission,* Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM(2021) 206 final, p. 3.

30 *Ranchordas,* Experimental Regulations for AI: Sandboxes for Morals and Mores, available at: https://ssrn.com/abstract=3839744 (18/10/2022).

31 *Bradford,* NULR 2012/1, p. 3.

32 *Bradford*, p. 25, 64.

- "ensure that AI systems placed on the Union market and used are safe and respect existing law on fundamental rights and Union values;
- ensure legal certainty to facilitate investment and innovation in AI;
- enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems;
- facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation."[33]

While these high-level objectives might neither be surprising nor particularly controversial, there continues to be lots of discussion whether the general direction of the 85 Articles and 9 Annexes that constitute the AIA draft proposal is appropriate in the first place. Most fundamentally, scholars such as *Kaminski* and *Edwards* raise the question if rather than once again applying traditional risk management mechanisms in an AI regulation context, new legal frameworks should contain more innovative mechanisms, such as emphasising public participation,[34] a stronger focus on harms suffered by specific groups rather and individuals, or "citizens juries."[35]

I. Risk-based approach

Probably the most prominent characteristic of the draft AIA act is a strong emphasis of the precautionary principle, which can be traced back to literature discussing ethics for technified/datafied societies, such as *Hans Jonas*' 1979 book "Prinzip Verantwortung" (principle of responsibility).[36] This thinking manifests in a risk-based approach framework with four categories for the application of AI systems:[37]

i. Unacceptable risk; with a ban of the use of the specific applications as consequence, although this is questionable when looking at the text in detail which will be done below.
ii. High risk; with comprehensive legal duties and recording obligations for "AI providers" to mitigate them.[38]

33 *European Commission,* Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM(2021) 206 final, p. 3.
34 *Kaminski*, Regulating the Risks of AI, available at: https://ssrn.com/abstract=4195066 (18/10/2022).
35 *Edwards*, Regulating AI in Europe: four problems and four solutions, p. 16, available at: https://www.adalovelaceinstitute.org/wp-content/uploads/2022/03/Expert-opinion-Lilian-Edwards-Regulating-AI-in-Europe.pdf (18/10/2022).
36 *Jonas,* p. 36.
37 A more comprehensive explanation with some concrete examples given by the Commission can be found at: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai (18/10/2022).
38 Art. 3(2) of the draft AIA contains a definition of provider that seems to encompass both private and public parties. It states: "'provider' means a natural or legal person, public authority, agency or other body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge;".

iii. Limited risk; which results in certain transparency obligations.
iv. Minimal or no risk.

In its current form and keeping the economic incentive in mind, the AIA is not generally aimed at prohibiting the use of AI in specific areas. However, when it comes to "unacceptable risk" the scenarios outlined in Art. 5(1) of the AIA draft are intended to prohibit certain uses, such as:

- use of subliminal techniques beyond a person's consciousness causing or likely causing a change of behaviour that causes physical or psychological harm to that person, or another person;
- placing on the market, putting into service or using an AI system that exploits vulnerabilities of a specific group of persons which ultimately also leads to physical or psychological harm;
- placing on the market, putting into service or use of AI systems by public authorities that establish social scoring practices, rating the behaviour of persons or groups;
- use of 'real time' biometric identification systems in publicly accessible spaces for law enforcement purposes, with the *exceptions* of
  - targeted searches for specific potential victims of crime;
  - prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons, or of a terrorist attack;
  - detection, localisation, identification or prosecution of a perpetrator or suspect of a criminal offence with a crime that is punishable by a custodial sentence or detention order of at least three years.[39]

The precise contents and included applications in this paragraph and category will be discussed heavily and controversially before the proposal is finally passed by the European legislators. To consider the first two scenarios of banning AI applications briefly, the formulations seem rather general, and it is difficult to clearly understand what the Commission is pointing at when using concepts such as "change of behaviour", or "exploiting vulnerabilities of a specific group". If the provisions remain this vague, it might be necessary for the Court of Justice to intervene and clarify the applicability and specific meaning through case-law, which will create legal uncertainty and take years.

When it comes to the prohibition of social scoring in the third scenario, it needs to be considered that credit-scoring and the prediction of creditworthiness are classified as high-risk applications of AI according to recital 37 of the draft AIA. Hence, these specific scoring practices are allowed applications of AI use. In consequence, this raises the question to which degree the AIA comprehensively bans all kinds of social scoring practices in the EU, since many of the known systems for

39 For the exact formulations see *European Commission,* Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM(2021) 206 final, p. 43, 44.

social scoring/"social credit" known from countries such as the PRC—one of the frontrunners of this practice—typically heavily depend on credit-scoring in the private sector, eventually and gradually expanding the data sources from there to increase the comprehensiveness of the citizen trustworthiness score.[40] A similar scenario seems imaginable in the EU, when combining the increasing financial transaction data with other means of profiling, such as interaction with e-government services. In conclusion, whether the AIA can effectively prohibit such practices with the substantive scope and nature of the regulation seems doubtful.

Finally, the last scenario relates to banning the use of real time biometric identification such as facial recognition. The way the provision is currently designed, it seems highly likely that the necessary infrastructures to deploy real time biometric identification in the exceptional scenarios where it is allowed (e.g. searching for a missing child), will permanently be put in place in crowded locations such as airports, metro stations, or football stadiums. This creates the risk that without very stringent oversight and control, these very capable infrastructures will be (ab-)used for tasks they were originally not intended for. Civil society organisations such as European Digital Rights (EDRi) have launched a public campaign to bring attention to the issue and comprehensively ban facial recognition to monitor public spaces in Europe. However, the formal European Citizen's Initiative corresponding to the campaign ultimately did not receive enough signatures to be further considered by EU institutions.[41]

Moving on, most of the attention and space in the draft AIA is taken up by the provisions associated with the "high risk" category. The AIA comes with two Annexes (II, III) that more specifically define the category. Whereas Annex II consists of a list of Union harmonisation legalisation that is based on the New Legislative Framework (NLF) and other Union harmonisation legislation, Annex III corresponds to Art. 6(2) of the draft AIA and aims at systems covering the following eight areas:[42]

- 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 and enjoyment of essential private and public services;
- Law enforcement in cases such as making individual risk assessments or detect the emotional state of a person, or applications such as Predictive Policing;

40 *Chen/Grossklags*, Social Sciences 2022/6, p. 2.

41 Nevertheless, the campaign has certainly sparked a lot of political debate and it remains to be seen how this will be reflected in the European Parliament and Council negotiations. See https://reclaimyourface.eu/ (18/10/2022) and https://europa.eu/citizens-initiative/initiatives/details/2021/000001_en (18/10/2022).

42 *European Commission,* Annexes to the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM(2021) 206 final, p. 4–5.

- Migration, asylum and border control management;
- Administration of justice and democratic processes.

Annex III contains several examples and general descriptions for what the eight categories contain more specifically, but also here it can be expected that the final AIA will contain many changes and clarifications. *Veale* and *Zuiderveen Borgesius* heavily criticise the draft AIA for following the standardisation approach along the NLF, which is essentially the same framework that is used to certify the safety of elevators, toys, or face masks in the EU. They argue that following this established EU framework places too much trust in the AI providers that have the main responsibility to guarantee the implementation of a Risk Management System (Art 9), Data and data governance regime (Art 10), Technical documentation (Art 11), Record-keeping (Art 12), etc. when it comes to high-risk AI systems as outlined in Art 16 of the draft AIA. As many rights and freedoms are at stake, they call for a more meaningful engagement of affected communities and public representation when standardising and certifying AI systems. Furthermore, they seem to question the democratic legitimacy of outsourcing complex negotiations around technical questions, which have implications for the realisation of human rights and public values, to technocratic expert and notifying bodies.[43]

This is understandable when considering the categories of AI use that so far seemed to gain the most attention in the public discussion, namely the regulation of AI use when it comes to unacceptable risks and high-risks. However, the European Commission argues that it sees its role mostly as facilitator of trustworthy AI development and use, and that in most cases providers of AI systems will have to comply with the transparency obligations associated with the limited risk or minimal risk category.[44] Here the Commission gives examples such as chatbots, or AI-enabled video games and spam filters.

II. Conformity and Impact Assessments

The AIA also builds on the trend to holistically consider consequences of the use of technology before placing it on the market, or putting it into service, or after substantially modifying an existing AI system. This includes both reflection of the consequences of use beyond the impact on the enjoyment of individual rights (e.g. including ethical and moral considerations, or the impact of the use of a system on a group), as well as the actual human-machine interaction in specific contexts (e.g. use of AI by law enforcement to detect a weapon hidden by a protester during a heated protest).

Through Art. 35 already the GDPR makes it mandatory for the data controller to carry out a data protection impact assessment (DPIA) if new technologies are being used, which are likely to result in high risk to the rights and freedoms of natural

43 *Veale/Zuiderveen Borgesius,* CRi 2021/4, p. 102–106.
44 See https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai (18/10/2022).

persons.[45] Similarly, the draft AIA requires to carry out "conformity assessments" for high-risk AI systems with the objective to mitigate the risks for "health, safety and fundamental rights."[46] The conformity assessment relates to technical documentation, record-keeping in the form of automatic recording of events, transparency and provision of information to users, human oversight of the system, as well as guaranteeing robustness, accuracy and cybersecurity of the AI system.[47] Primarily this is an obligation of the provider of a high-risk AI system, but it can also be carried out by other parties such as the manufacturer or distributor, among others.[48]

One of the main criticisms relating to GDPR DPIAs is that the text of the 2016 regulation itself remains rather vague when it comes to the concrete methodology that should be applied. Over the years this gap has been filled with practitioner's manuals,[49] as well as guides developed by public institutions such as the national data protection of France (CNIL) and the German data protection authorities (e.g. ULD Schleswig-Holstein).[50] Similarly for AI specifically, literature is emerging that discusses Human Rights, Ethical and Social Impact Assessments (HRESIA proposed by *Mantelero*),[51] as well as holistic processes used to evaluate the trustworthiness of AI-based technologies at different stages of the AI lifecycle (Z-Inspection by *Zicari* et al.).[52] One can only hope that these and similar initiatives eventually pave the way to more inclusive and interdisciplinary ways of designing and using AI systems.

III. Complex Enforcement and Oversight

While conformity assessments are already a form of ex-ante regulation of AI systems, currently there seems to be a more general discussion on the appropriate balance between mechanisms which would allow for ex-ante control of AI and the supervision and ex-post oversight, as well as sanctioning. For instance, *Malgieri* and *Pasquale* propose an approach of "unlawfulness by default", where some AI developers have the burden of proof to demonstrate that their systems are not creating

45 For a more detailed discussion see *Kosta*, in: Kuner/Bygrave/Docksey (eds.), Art. 35 GDPR.

46 *European Commission,* Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM(2021) 206 final, recital 43.

47 *Demetzou,* Introduction to the Conformity Assessment under the Draft EU AI Act, and how it compares to DPIAs, available at: https://fpf.org/blog/introduction-to-the-conformity-assessment-under-the-draft-eu-ai-act-and-how-it-compares-to-dpias/ (18/10/2022).

48 Ibid.

49 See e.g. *Martin/Friedewald* et al.

50 See https://www.cnil.fr/en/privacy-impact-assessment-pia (18/10/2022). The "Standard Data Protection Model" of the Unabhängiges Landeszentrum für Datenschutz Schleswig Holstein is even slightly broader in the approach, available at: https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methodology_V2.0b.pdf (18/10/2022).

51 *Mantelero*, p. 15–32.

52 *Zicari* et al., How to Assess Trustworthy AI in Practice, available at: https://doi.org/10.48550/arXiv.2206.09887 (18/10/2022).

harms such as discrimination, unfair decisions, or inaccurate results before even being allowed on the market.[53]

Enforcement is certainly a key aspect of the AIA, and it remains to be seen which lessons the European legislators will learn from the GDPR. While the GDPR established the possibility to levy unprecedented sanctions for data protection violations, it is also well established that the European and national supervisory authorities are overburdened/underfunded,[54] and that the coordination among them is complex.[55] However, there is not much reason to be optimistic the AIA supervisory and enforcement regime will become simpler and more straightforward. Apart from putting the burden of proof for compliance on providers of AI systems and the bodies they use for certifying compliance with the AIA,[56] according to Art. 59 draft AIA Member States have an obligation to establish or designate a (or in seemingly exceptional organisational and administrative reasons more than one) national supervisory authority. This supervisory authority acts as notifying and market surveillance authority.[57] It will typically collaborate with other national competent authorities, which probably will have more expertise in handling a specific subject or sector. The national authorities will be coordinated in a newly established "European Artificial Intelligence Board" (Art. 56 draft AIA), which will provide advice and assistance to the Commission that will chair the board according to the draft. The national supervisory authorities have a duty to report to the Commission regarding their supervisory activities, and the European Data Protection Supervisor will also join the board.

This latter aspect hints at a major question emerging from the proposed supervision structure: How will the relation between supervision of already existing regimes such as the GDPR – which has applicable provisions to some forms of AI use, such as the review of automated-decision making in Art. 22 GDPR – and the newly established AIA structure look like and work in practice? While GDPR is the most obvious example, the same question might be asked for those parts of frameworks such as the DSA and DSM, which could become relevant for specific aspects of AI Governance in the EU. Besides the discretion for self-certification of

53 *Malgieri/Pasquale,* From Transparency to Justification: Toward Ex Ante Accountability of AI, available at: https://ssrn.com/abstract=4099657 (18/10/2022).

54 The 2021 annual report of the European Data Protection Board states on p. 82: "The vast majority of Supervisory Authorities (22) explicitly stated that their allocated budget is not sufficient for carrying out the work activities. Based on the information from 29 Supervisory Authorities from EEA countries before August 2021, six Supervisory Authorities even faced a budgetary decrease in comparison to their 2020 budget." Available at: https://edpb.europa.eu/system/files/2022-05/edpb_annual_report_2021_en.pdf (18/10/2022).

55 See as an example the recent dispute between the French and Polish supervisory authority on the height of a fine levied against a large hotel chain, which eventually was settled in August 2022 according to the dispute resolution mechanism in Art. 65 GDPR. Available at: https://edpb.europa.eu/news/news/2022/edpb-publishes-art65-gdpr-dispute-resolution-binding-decision-concerning-accor-sa_en (18/10/2022).

56 *Veale/Zuiderveen Borgesius,* CRi 2021/4, p. 106.

57 Although there seem to be sector exceptions for supervision according to Art. 63 draft AIA. They relate to the financial sector and others.

AI providers and the factual position of notifying bodies such as technical standardisation bodies, the vectors that matter here are the degree of centralisation and decentralisation of the supervision system – currently the Member States seem to have quite large discretion, which might be worrisome if coupled with different national aspirations in AI use and influence of the technology sector for the economy – as well as the integration of the AIA oversight system with other existing regimes.

When it comes to penalties, Article 71 draft AIA foresees fines up to 30 Mill. Euros or, if the offender is a company, 6% of its worldwide annual turnover for the preceding financial year for companies using AI systems which are banned according to Art. 5 draft AIA, or non-compliance with Art. 10 draft AIA relating to data and data governance (e.g. not documenting and clearly explaining design choices, data collection, examination in view of possible biases, etc.). For violation of all other articles of the AIA fines up to 20 Mill. Euros are possible, or if the offender is a company, 4% of its worldwide annual turnover for the preceding financial year. The supply of incorrect, incomplete, or misleading information to notifying bodies involved in the certification process according to the NLF can be fined with 10 Mill. Euros or 2% of the worldwide annual turnover in the case of companies. Finally, Art. 72 draft AIA foresees a specific provision for administrative fines against EU institutions, agencies and bodies which are under the supervision of the European Data Protection Supervisor.

D. The 'Brussels Effect' versus Human Dignity?

There are many remaining aspects worth analysing when it comes to the AIA and the Commission proposal from April 2021. However, it goes beyond of the scope of this article to discuss them all in detail. Before concluding, with an eye to exploring the main question of this article, this section will briefly consider the current regulatory dynamics around the AIA within and outside the EU, focusing mostly on the legal architecture and consequences of developments in other influential states and international organisations for the manifestation of the Brussels Effect.

I. The AIA from within the EU

As already briefly mentioned, the AIA does not stand in and of itself. On the one hand, it is part of a wider "European approach to AI",[58] which ranges from the establishment of ethical principles for trustworthy AI to investment strategies. On the other hand, other legal frameworks such as the GDPR, DSA, DSM, or the already existing product harmonisation frameworks as mentioned in Annex II are of relevance to get the full picture of AI regulation in the EU. It would be quite surprising if all these emerging and existing frameworks would result in a harmonious and

58 *European Commission*, A European approach to artificial intelligence, available at: https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence (18/10/2022).

consistent governance of AI in the EU from the outset, once they are all developed and in force. At the same time, this does not seem to make it less likely that the political negotiations around the AIA will take considerably more time. On 3 May 2022 the European Parliament published a press release stating that members see huge benefits of using AI to address climate change, the management of pandemics, as well as increased chances for the labour market. At the same time, they warn of risks for fundamental rights such as privacy. They also note that the EU has fallen behind in the global race for tech leadership.[59] Corresponding to this ambition of the Parliament, the Czech Council presidency has made AI regulation one of its priorities for the second half of 2022.[60] Although the EU faces many geopolitical challenges, it would not be entirely surprising to have the negotiations around the AIA at a very advanced state in the second half of 2023, even potentially finished.

What will be interesting during this time is whether the next versions of the legal text will still contain prominent aspects of delegation of powers to the Commission such as with the chairing of the EU AI Board, or the extensive use of Annexes to describe and interpret key concepts of the framework. This contains the danger that democratic processes will be undermined on the one hand. On the other hand, it is also a way to centralise power and make policies more flexible and consistent. At the same time, without a significant revision of the EU treaties, the AIA will not have any influence on national security in the EU beyond law enforcement, leaving the much-discussed domain of military application of AI systems open to the discretion of Member States and negotiations in other international fora such as the United Nations.[61]

II. The AIA from outside the EU

While the AIA seems to receive much attention, it should not be overlooked that similar work is going in other institutions and countries. The Council of Europe has a comprehensive initiative to work on binding and non-binding international agreements relating to AI use. As of 2022 a dedicated Committee on AI (CAI) has started its work, which builds its activities on an ad-hoc Committee (CAHAI) that was already active since 2019. Many issues are being explored and covered, such as AI use with regards to privacy and data protection, justice and public administration,

59 *European Parliament*, Artificial intelligence: MEPs want the EU to be a global standard-setter, available at: https://www.europarl.europa.eu/news/en/press-room/20220429IPR28228/artificial-intelligence-meps-want-the-eu-to-be-a-global-standard-setter (18/10/2022).

60 *Czech Presidency of the Council of the European Union*, Priorities, available at: https://czech-presidency.consilium.europa.eu/en/programme/priorities/ (18/10/2022). A positioning paper from 15 July 2022 is available at: https://data.consilium.europa.eu/doc/document/ST-11124-2022-INIT/en/pdf (18/10/2022).

61 *Blauth/Gstrein/Zwitter,* IEEE Access 2022, p. 77117.

healthcare and biomedicine, non-discrimination and gender equality, social rights, education, children's rights, as well as freedom of expression and culture.[62]

When it comes to regulatory activities in globally influential countries in the domain, several initiatives can be identified in the United States. Specifically, there is discussion around a US Algorithmic Accountability Act of 2022 (US AAA) suggested by Senators Ron Wyden and Cory Brooker, as well as Representative Yvette Clark on 3 February 2022.[63] The US AAA and AIA seem to have some elements in common as they both establish ex-ante compliance mechanisms such as impact assessments, as well as requiring increased transparency.[64] Overall however, the AAA seems less detailed and ambitious than the AIA. At the same time, it remains to be seen how much traction the proposal will ultimately gain in a politically very polarised landscape.[65] *Kaminski* further discusses the U.S. Department of Commerce's National Institute of Standards and Technology (NIST)'s emerging Risk Management Framework, as well as a bill discussed in Washington State (SB 5116), which seems particularly promising in terms of public participation.[66] While democratic countries need time to deliberate on regulation, the PRC has recently enacted regulation relating to the use of AI in the private sector. As of March 2022, the way online recommendations on webpages and apps are generated through algorithms, suggesting what to buy, watch or read are subject to government control.[67] This can be seen in the context of a broader push of the political leadership to control AI in the private sector, and an attempt of Beijing to become an influential standard-setter for emerging technologies.[68]

E. Outlook and Conclusion

Has the EU chosen an approach for AI regulation that emphasises standard setting and political influence leveraging the 'Brussels Effect', therefore de-prioritising the protection and promotion of human dignity and human rights? After considering the main objectives and characteristics of the draft AIA in context, it remains im-

62 For an overview and latest updates see *Council of Europe*, Council of Europe and Artificial Intelligence, available at: https://www.coe.int/en/web/artificial-intelligence/home (18/10/2022).

63 *Office of Ron Wyden,* Wyden, Booker and Clarke Introduce Algorithmic Accountability Act of 2022 To Require New Transparency And Accountability For Automated Decision Systems, available at: https://www.wyden.senate.gov/news/press-releases/wyden-booker-and-clarke-introduce-algorithmic-accountability-act-of-2022-to-require-new-transparency-and-accountability-for-automated-decision-systems (18/10/2022).

64 *Mökander/Juneja/Watson/Floridi*, p. 2.

65 Ibid., p. 5–6.

66 *Kaminski*, Regulating the Risks of AI, available at: https://ssrn.com/abstract=4195066 (18/10/2022), p. 54–75.

67 *Qu,* China's algorithm law takes effect to curb Big Tech's sway in public opinion, available at: https://www.scmp.com/tech/policy/article/3168816/chinas-algorithm-law-takes-effect-curb-big-techs-sway-public-opinion (18/10/2022).

68 *Espinoza/Pop*, EU to outline tech standards plan to counter China influence, available at: https://on.ft.com/3wVuR7n (18/10/2022).

possible to give a simple Yes or No answer to this question at this point. After all, the proposal seems to draw from many – potentially too many – different traditions and aspects of EU law, such as the NLF product standardisation approach, human rights inspired bans and traditional risk mitigation mechanisms to heavily regulate certain uses of AI in the hope to protect citizens from potential harms, innovation incentives and regulatory sandboxes, as well as many others. It also seems premature to conclude on the main question explored in this article, since the legislative negotiations on the AIA take place at a breath-taking speed during the time this article has been written, as deliberations are going on in parallel in the European Parliament and the Council.[69]

However, regardless of the outcome the AIA will have to integrate as only one voice in a chorus of regulatory frameworks addressing AI development and deployment in the EU. Other regulations and directives such as the GDPR, DSA and DSM are already in force, or currently under negotiation. Furthermore, it remains to be seen which initiatives around and outside the EU will impact AI development and deployment in Member States, and it seems unlikely that in sectors on the margin of EU competence—such as national security—there is much that the Union in its current form can do to regulate and govern matters.

Is the work on the AIA therefore pointless, doomed to produce a legal regulation that heads into multiple inconsistent directions at the same time? Probably the most relevant achievement of the AIA to date might be its pioneering role, which enables society to have a serious discussion about AI regulation in general. This in itself has an impact on many areas of society, also beyond the borders of the EU. While it is highly unlikely that the AIA will become a flawless legal framework whenever it is finished, it addresses a gap in regulation that is perceived as illegitimate and dangerous by many. At this point one can only hope that the regulators will compromise on a final version of the AIA that reduces most of the potential harms AI systems—as well as the AIA itself—can cause, eventually enabling AI development and application in a way that promotes human dignity and broad societal welfare.

Bibliography

BLAUTH, TAÍS FERNANDA; GSTREIN, OSKAR JOSEF; ZWITTER, ANDREJ, *Artificial Intelligence Crime: An Overview of Malicious Use and Abuse of AI*, IEEE Access, 2022, vol. 10, p. 77110–77122

BORGES FORTES, PEDRO; BAQUERO, MARECELLO PABLO; RESTREPO AMARILES, DAVID, *Artificial Intelligence Risks and Algorithmic Regulation*, European Journal of Risk Regulation, 2022, p. 1–16

BRADFORD, ANU, *The Brussels Effect*, Northwestern University Law Review, 2012, vol. 107(1), p. 1–68

69 For the current state see the procedure in the legislative observatory, available at: https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2021/0106(COD)&l=en (18/10/2022).

BRADFORD, ANU, *The Brussels effect: How the European Union rules the world*, Oxford, 2020

BURGGRAF, JÜRGEN; GERLACH, CHRISTINE; WIESNER, JAN, *EU Digital Services und Digital Markets Act – Wie die EU die Internet-Ökonomie regulieren will*, Media Perspektiven, 2021, Issue 5, p. 292–300

BYGRAVE, LEE A., *Article 22 GDPR*, in: Kuner, Christopher; Bygrave, Lee A.; Docksey, Christopher A. (eds.), The EU General Data Protection Regulation (GDPR): a commentary, Oxford, 2020, p. 522–542

CHEN, MO; GROSSKLAGS, JENS, *Social Control in the Digital Transformation of Society: A Case Study of the Chinese Social Credit System*, Social Sciences 2022, vol. 11(6), p. 229 ff.

CRAWFORD, KATE, *Atlas of AI*, New Haven and London, 2021

DEAN, JEFFREY, *A Golden Decade of Deep Learning: Computing Systems & Applications*, Daedalus, 2022, vol. 151(2), p. 58–74

GONZÁLEZ FUSTER, GLORIA, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Governance and Technology Series, vol 16., Cham, 2014

GREENLEAF, GRAHAM, *Now 157 Countries: Twelve Data Privacy Laws in 2021/22*, Privacy Laws & Business International Report, 2022, vol. 176(1), p. 3–8

GSTREIN, OSKAR JOSEF; BEAULIEU, ANNE, *How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches*, Philosophy and Technology, 2022, vol. 35(3), p. 1–38

GSTREIN, OSKAR JOSEF; BUNNIK, ANNO; ZWITTER, ANDREJ, *Ethical, Legal and Social Challenges of Predictive Policing*, Católica Law Review, 2019, vol. 3(3), p. 77–98

GSTREIN, OSKAR JOSEF; ZWITTER, ANDREJ, *Een transparant debat over algoritmen*, Bestuurskunde, 2020, vol. 29, p. 30–42

GSTREIN, OSKAR JOSEF; ZWITTER, ANDREJ, *Extraterritorial application of the GDPR: promoting European values or power?*, Internet Policy Review, 2021, vol. 10(3), p. 1–30

HANER, JUSTIN, GARCIA, DENISE, *The Artificial Intelligence Arms Race: Trends and World Leaders in Autonomous Weapons Development*, Global Policy Volume, 2019, vol. 10, p. 331–337

HILDEBRANDT, MIREILLE, *Algorithmic regulation and the rule of law*, Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 2018, vol. 376(2128)

JONAS, HANS, *Das Prinzip Verantwortung. Versuch einer Ethik für die technologische Zivilisation*, Frankfurt am Main, 1979

KOSTA, ELENI, *Article 35 GDPR*, in: Kuner, Christopher; Bygrave, Lee A.; Docksey, Christopher A. (eds.), The EU General Data Protection Regulation (GDPR): a commentary, Oxford, 2020, p. 665–679

LARSSON, STEFAN; HEINTZ, FREDRIK, *Transparency in artificial intelligence*, Internet Policy Review, 2020, vol. 9(2), p. 1–16

MANTELERO, ALESSANDRO, *Beyond Data – Human Rights, Ethical and Social Impact Assessment in AI*, The Hague, 2022

MARTIN, NICHOLAS; FRIEDEWALD, MICHAEL et al., *The Data Protection Impact Assessment According to Article 35 GDPR. A Practicioner's Manual,* Karlsruhe, 2020

MILAN, STEFANIA, *Techno-solutionism and the standard human in the making of the COVID-19 pandemic*, Big Data & Society, 2020, vol. 7(2), p. 1–7

MOROZOV, EVGENI, *To Save Everything, Click Here*, Reprint edition, New York, 2014

MÖKANDER, JAKOB; JUNEJA, PRATHM: WATSON, DAVID S.; FLORIDI, LUCIANO, *The US Algorithmic Accountability Act of 2022 vs. The EU Artificial Intelligence Act: what can they learn from each other?*, Minds and Machines, 2022

NEMITZ, PAUL, *Constitutional democracy and technology in the age of artificial intelligence*, Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 2018, vol. 376(2133)

OLSEN, HENRIK PALMER; LIVINGSSTON SLOSSER; JACOB, TROELS; HILDEBRANDT, THOMAS, *What's in the Box? The Legal Requirement of Explainability in Computationally Aided Decision-Making in Public Administration*, in: Micklitz, Hans-W., et al. (eds.), Constitutional Challenges in the Algorithmic Society, Cambridge, 2021, p. 219–235

TAYLOR, LINNET, *Can AI governance be progressive? Group interests, group privacy and abnormal justice*, in: Zwitter Andrej; Gstrein, Oskar Josef (eds.), Handbook on the Politics and Governance of Big Data and Artificial Intelligence, Cheltenham, forthcoming 2023

TAULLI, TOM, *Artificial Intelligence Basics*, New York, 2019

VEALE, MICHAEL, ZUIDERVEEN BORGESIUS, FREDERIK, *Demystifying the Draft EU Artificial Intelligence Act*, Computer Law Review International, 2021, vol. 22(4), p. 97–112