Piercing the Westphalian Veil: Assessing the Liability for AI-Driven Harms

Syed Suliman Ali[1], Nazli Ismail Nawang[2*], Mohd Badrol Bin Awang[3]

[1]PhD Law Student, Faculty of Law and International Relations, Universiti Sultan Zainal Abidin (UniSZA), Terengganu, Malaysia

[2]Associate Professor, Faculty of Law and International Relations, Universiti Sultan Zainal Abidin (UniSZA), Terengganu, Malaysia

[3]Associate Professor, Faculty of Law and International Relations, Universiti Sultan Zainal Abidin (UniSZA), Terengganu, Malaysia

Corresponding Author: Nazli Ismail Nawang, inazli@unisza.edu.my

HOW TO CITE:

Syed Suliman Ali, Nazli Ismail Nawang, Mohd Badrol Bin Awang (2026). Piercing the Westphalian Veil: Assessing the Liability for AI-Driven Harms. International Journal of Special Education, 41(10s), 1414-1422

COPYRIGHT STATEMENT:

Copyright: © 2026 Authors. Open access publication underthe terms and conditions of the Creative CommonsAttribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).

ABSTRACT:

Provide As autonomous AI systems outpaced traditional Westphalian legal frameworks, a global Enforcement gap has emerged, leaving non-state-driven harm largely unchecked by international law. This article explores the imperative transition from ethical soft law to binding law accountability. The primary objective is to propose a Binding International AI Liability Protocol (IALP) under the 2025 UN Global Digital Compact, utilising the technical architecture of the EU AI Act and the Product Liability Directive (2024/2853). Employing a doctrinal research methodology, the study analyses the EU's strict liability standards and the presumption of defectiveness as normative archetypes for global accountability. This research is significant as it provides a blueprint for bridging the digital-liability divide, ensuring victims in the Global South are protected from cross-border algorithmic harm. It concludes that by multilateralizing the EU's liability regime through a UN-anchored agency, the international community can establish a universal social contract that holds multinational corporations directly accountable. Without this binding transition, global AI governance will remain fragmented, leaving human rights vulnerable to the functional sovereignty of tech giants.

Keywords: EU AI Act; Product Liability Directive (EU) 2024/2853; UN Global Digital Compact; Non-State Actors; Algorithmic Accountability; Brussels Effect

1. Introduction

The year 2025 is a Constitutional Moment for the governance of Artificial Intelligence (AI). While the global community has spent the last decade navigating a sea of fragmented ethical guidelines and non-binding soft law declarations, the European Union has moved decisively into the active enforcement phase of the AI Act (Regulation (EU) 2024/1689) (EU AI Act, 2024). As of August 2025, the world got an official start to obligations for General-Purpose AI (GPAI) models, and this is not just a theoretical debate; bold regulatory control is now in effect. By operationalising the European AI Office and enforcing bans on unacceptable risk practices, such as social scoring and exploitative biometric categorisation, the EU has effectively turned its internal market standards into a global standard

and benchmark for algorithmic safety (Maslej et al., 2025).

However, a basic structural issue remains in place in the current international legal order. Traditional international law is stubbornly State-Centric and based on a Westphalian model by which disputes are mediated principally between sovereign states. In contrast, the greatest harm of AI is Non-State Driven, the orchestration of a few multinational corporations (MNCs) who are functionally sovereign over digital ecosystems. While the EU's unilateral regulatory reach, or the widely used term of the Brussels Effect, has had the effect of forcing global tech giants to shape the internal architecture of their businesses to match up with their European values, this influence remains geographically limited. It is not enough to shelter victims in the Global South when there is a lack of domestic enforcement capacity combined with the high costs of conformity assessments, which constitute a Liability Divide. Without a multilateral framework, the Brussels Effect could degenerate into a sort of digital paternalism, instead of proving to be a tool of global justice (UN Charter, 1945).

This article will argue that the internal technical and legal consistency of the EU's burgeoning liability regime, when coupled, for instance, with the Revised Product Liability Directive (EU) 2024/2853, does provide the necessary architectural foundation for a binding United Nations treaty (Directive [EU] 2024/2853, 2024). Based on the synthesis and alignment of the EU's risk-based classifications and the 2025 UN Global Digital Compact (GDC) implementation roadmap, this study proposes establishing an International AI Liability Protocol (IALP) (United Nations, 2024). This protocol would go beyond state-mediated responsibility for setting up a direct, binding accountability mechanism with the non-state providers of AI. Only by multilateralising the EU's gold standard through an UN-anchored protocol can the international community ensure global regulatory uniformity, the racial availing of jurisdictional arbitrage and equal redress for AI-driven harms within an increasingly borderless digital world (Leonetti & Pecoraro, 2025).

3. Theoretical Framework: Transnational Legal Accountability

The established paradigm of Westphalia, based on territorial sovereignty and state mediation, is very outdated in the context of the new borderless algorithmic reality (UN Charter, 1945). In this digital age, the binary distinction of these two types of actors, public and private, has melted and been replaced with a condition known by scholars as Functional Sovereignty. Large-scale AI providers and tech giants no longer offer tools; they control digital territories, how we discuss issues and control the operation of important infrastructure, thereby exerting influence that is traditionally passed on to the state. This functional sovereignty has enabled non-state actors to influence the legal and social realities of millions without democratic safeguards or checks and balances that are inherent in the constitutional framework of the nations. As these types of entities operate across jurisdictions, they play on the Regulatory Rift, which is an alignment of systemic regulatory laws between fragmented national laws: essentially, traditional territorial law is an insufficient tool of accountability. To remedy this, the field of Societal Constitutionalism proposes that if private actors are going to exercise powers that are like public powers, then they should have to be subject to constitutional-grade limitations that transcend national borders (Niazi, 2025).

To address this vacuum, this research considers a concept of Social Contract for the Digital Age, i.e., a normative framework promoted by the UN Global Digital Compact (GDC) in the UN Global Digital Compact implementation phases of 2024 and 2025 (United Nations, 2024). This renewed social contract assumes that the exponential change of AI requires a tripartite agreement between states, citizens and private enterprises. Under this model, the legitimacy of the operation of a non-state actor depends on the acceptance of direct legal responsibility. Unlike the 20th-century model of State Responsibility, in which international law did not cover

corporations except through the vehicle of their respective home states, under the Digital Social Contract, the imposition of Direct International Liability is justified. It posits that since the providers of AI have global influence and possess the technical power to mitigate risk at the source, they should be bound to a global Safety Floor - a set of binding requirements that follow the technology across borders, whatever the entity may be headquartered in and wherever the harm occurs (International Law Commission [ILC], 2001).

This is a theoretical shift that has been highly informed by the EU's pioneering approach to Extraterritorial Accountability (EU AI Act, 2024). By addressing high-risk AI as a systemic product, rather than as a service, the EU has created the means for a transnational mechanism of accountability using the Brussels Effect. The shift from Soft Law ethics - including the voluntary principles of an early version of the UN guidelines - to the Hard Law of the International AI Liability Protocol (IALP) is based on this new social contract (UNESCO, 2021). It recognises that in a world run by algorithms, justice cannot be enforced within the boundaries of nations; when this happens, Liability Gaps are created where victims are rendered without any recourse against developers based in other countries. Instead, accountability needs to be transnational by design, meaning that non-state actors are not only held dynamically accountable but also held liable for systemic harms with UN-appearing multilateralism (Erman & Furendal, 2025).

This framework successfully develops the internal liability standards the EU itself promotes to Cancun, namely, the principle of strict liability for high-risk systems, into an international imperative that guarantees the Social Contract will be enforced not only by individual countries, but by an international legal order that acts collectively and is focused on human dignity rather than jurisdictional technicalities (Directive [EU] 2024/2853, 2024).

4. Deconstructing the EU Accountability Design: The 2024-2025 Surge:

The present European legal environment is not just an exercise in ethics but a highly structured, two-track enforcement regime. This structural design consists of two main pillars: the AI Act (Regulation (EU) 2024/1689), which contains ex-ante safety standards, and the New Product Liability Directive (Directive (EU) 2024/2853), which contains the ex-post-civil remedy. They constitute, in late 2025, a highly developed accountability structure in the world in the form of a virtual Brussels Standard, which non-State actors must follow if they do not want to lose their market access.

The most critical juncture in implementing the AI Act was reached in August 2025. On August 2nd, 2025, transparency obligations for General-Purpose AI (GPAI) models came into law, which regulates AI applications. Under the terms of Article 53, providers of GPAI models, such as foundation models, now have to ensure that they maintain technical documentation, inform downstream deployers, and most importantly, publish a detailed summary of the content used for training. To facilitate this, the European AI Office, created early in 2025, released the first GPAI Code of Practice in July 2025 (European AI Office, 2025). This Code is a quasi-regulatory bridge in that it sets out the specific metrics around Safety and Security and Copyright Compliance that must be met by providers that wish to show they are in line with their compliance with the Act.

At the same time, the year 2025 has witnessed the concretisation of High-Risk Conformity Assessments. While the deadline for the full enforcement of high-risk systems is August 2026, the European AI Office and the Scientific Panel of Independent Experts have been busy working on standardising the conformity assessments required for systems used in critical sectors such as education, employment and law enforcement during 2025. These assessments have the providers implementing strict Risk Management Systems (Article 9) and Data Governance (Article 10) (EU AI Act, 2024). For a research article, the

significance is that these mandatory safety requirements have now become the yardstick for civil law for determining whether a system is defective.

The biggest and most facilitating development in 2025 is the transposition of the New Product Liability Directive (2024/2853) (Directive [EU] 2024/2853, 2024). This directive fundamentally modernises the regime in place in 1985 by explicitly including Software, including standalone systems with artificial intelligence (AI) and connecting services, with the definition of a product (Article 4(1)). This is one of the main pieces of original data for this research, since it removes long-standing legal ambiguity on whether an intangible algorithm can be subject to strict liability (Council Directive 85/374/EEC, 1985).

Under this new regime, a provider is strictly liable, which means a victim does not even need to claim negligence or fault. Instead, the victim only has to demonstrate that the AI was defective, that they have been damaged and that a causal link exists. Relevantly, the 2025 legal framework adds to this definition a condition for medically recognised psychological harm as well as the destruction or corruption of data. Article 7 of the Product Liability Directive requires courts to consider defectiveness by looking at the ability of the AI system to continue learning after deployment and the cybersecurity vulnerabilities, in consideration of the dynamic and autonomous nature of modern AI. Furthermore, it makes a long stop of 25 years for latent personal injuries to bring the system a much-needed check on the long-term societal effects of biased or harmful AI. The real innovation that exists within the PLD, and the key recommendation of this article, is the Presumption of Defectiveness (Article 10). Recognising the problem of the Black Box, where, in its technical complexity, AI can make it excessively difficult for a consumer to prove a defect, the EU has introduced a rebuttable presumption. If a claimant can present a good case and demonstrate that the AI system was not compliant with the mandatory safety requirements of the AI Act (failure or lack of human oversight, or inadequate transparency of the training data, for example), the court assumes it is defective (Dawson, 2023).

This mechanism is effectively putting the burden of proof on the victim, instead of on the multi-billion-dollar provider. The provider then has to disclose necessary technical evidence (with the aid of court-ordered confidentiality) to demonstrate that the system was not defective. This research argues that this mechanism, the connection between regulatory non-compliance and an assumed liability, is the crucial bridge that must be taken up by the UN Global Digital Compact (GDC). For the Global South, where there may not be technical expertise to audit complex code, this presumption offers a self-dare to act procedurally to justice (Yilma, 2025). By adapting the Presumption of Defectiveness on a multilateral scale implementation map for the GDC by 2025, change can still be created at the UN by ensuring that the burden of technical overwhelm remains on the entity that gains profit from the technology and not the individual who gets injured by such a technology. This guarantees that data sovereignty has a liability sovereignty as well; this would enable the developed nations to enforce their rights against non-state actors without having to possess an equal indigenous technical auditing capability (Ishkhanyan, 2025).

5. Judicial Enforcement: CJEU 2025 Precedents

The enforcement of artificial intelligence accountability has moved from a theoretical requirement to a judicial reality thanks to this landmark jurisprudence of the Court of Justice of the European Union (CJEU). As of late 2025, the CJEU has stood on its own feet to become the global Constitutional Arbiter of algorithmic rights, no longer confined to the text of the AI Act and beyond the question of its enforceability for individuals (EU AI Act, 2024).

On February 27, 2025, the CJEU gave its final judgment in C-203/22 or Dun & Bradstreet Austria, a case that has become the Marbury v. Madison of the AI era. The conflict involved a legal firm in a credit score that used automated processing technology for negative credit scores,

resulting in a consumer's mobile contract application being summarily rejected. The Court's decision is revolutionary on two accounts. First, it confirmed the existence of the Right of Explanation as such, as an autonomous legal right under Article 15(1)(h) and Article 22 of the GDPR. The Court held that meaningful information about the logic involved requires that the controller give the data subject an explanation which is easy, clear and accessible (Ponce, 2025). Crucially, the CJEU held that the technical complexity of an algorithm black box excuse does not provide a relief to the provider of its duty to reduce the complexity in the explanation for the layman (GDPR, 2016).

Second, the Court discussed the conflict between Trade Secrets and Transparency. In a key ruling that will be the subject of one of the most infamous cases ever to go through the European Court of Justice, it has been deemed that intellectual property rights and trade secrets are not total and cannot be used as a blanket justification for opacity (Danila, 2025). The Court issued a Balancing Mandate, which permitted national courts and data protection authorities to see protected information in camera to ensure the fairness of the logic. This successfully subordinates proprietary profit-interests to the fundamental human right of due process (Dun & Bradstreet Austria, 2025).

The Dun & Bradstreet precedent defines the normative basis for a Binding International AI Court/enforcement body under the UN. If a regional court can successfully force multinational corporations to disclose the logic behind their proprietary models, then it is proof that a Judicial Shield against algorithmic harm is technically and legally possible.

This research argues for the EU's judicial model to be the blueprint of the International AI Liability Protocol (IALP). By lifting the automatically legally binding aim of the CJEU to the UN-led adjudicatory body, the international community will be able to ensure the implication of non-state actors to a universal standard of review (Chaudhuri, 2021). Such a body would address the Enforcement Gap, which persists in the Global South, in which national courts often do not have the technical expertise or domain jurisdiction to challenge global tech giants. The CJEU has proved that Secrecy without Oversight is no longer a viable legal defence, and the UN now needs to globalise this judicial oversight (Dun & Bradstreet Austria, 2025).

The EU judicial uptick in the implementation is not in a vacuum; it will be based on the Council of Europe Framework Convention on Artificial Intelligence (2024). As the world's first binding international treaty on AI, the Convention requires that all AI lifecycles must not condone human rights, democracy and the rule of law (Council of Europe, 2024).

This Convention has been made in the EU in formal adherence in Late 2024/2025, developed into a Living Instrument. Much like the European Convention on Human Rights (ECHR), the AI Framework Convention is starting to be interpreted by the CJEU in the light of conditions in the present day, namely, the emergence of generative AI and autonomous agents (ECHR, 1950). This Evolutive Interpretation helps to ensure that the law will not be out of date as technology changes.

By correlating the technical requirements of the AI Act with the human rights requirements of the Framework Convention, the EU has established a Unitary Legal Order. This article assumes that this integrated model - the one in which technical standards are enforced through a judicial system focused on human rights - is the only viable way forward for the UN Global Digital Compact (Bauer & Pandya, 2024). For the Global South, this transition allows AI to be regulated not just in terms of access to markets, but of human dignity and protection (protection and promotion of human rights) against the Functional Sovereignty of non-state actors (Malacka, 2024).

6. The Proposal: The International AI Liability Protocol (IALP)

The result of the above analysis is a proposal for a Binding International AI Liability Protocol (IALP). This protocol is aimed at bridging the gap between the internal architecture of liability in the EU and the global governance goals of the UN.

By shifting from a State-to-State model to an Agent to State / Individual model, the IALP accommodates this reality of the use of non-state actors as the main drivers of AI risk.

The administrative and enforcement core of the IALP must be some sort of centralised intergovernmental organisation: the International AI Agency (IAIA). In the role of the operational arm of the UN Global Digital Compact (GDC), the IAIA draws inspiration, conceptually, from the International Atomic Energy Agency (IAEA). However, while the IAEA's focus is on non-proliferation and safety, the verification, certification and liability enforcement would be the primary mandate of the IAIA on high-risk AI systems (United Nations, 2024).

The IAIA would be a Global Repository where any provider wishing to deploy a Systemic Risk model is required to register the technical documentation, like the requirements imposed by the EU on the registration of the AI Act (Annex-VII). This agency would not replace national regulators but will represent the final authority in the face of cross-border disputes and the certification of the Conformity Assessments for models which will be operated through multiple jurisdictions. For the Global South, the IAIA is a technical hub through which countries with limited resources on the continent will have access to the expertise needed to audit complicated algorithms so that no country is left behind in enforcing its own sovereignty (Revolidis, 2024).

The first pillar of the IALP follows the EU's tiered approach to risk, in the case of models, General-Purpose AI (GPAI) with systemic risk. Under the protocol, any non-state provider having an AI model that tops a predefined technical threshold, such as the EU's 1025 FLOPs computing power mark or important cumulative market reach, would be liable for Direct Strict Liability (Röttger, 2025).

This takes the burden off the victim to prove wrongfulness. Instead, if an AI system is the cause of medically recognised harm, property damage or catastrophic data loss, then the provider is liable by virtue of the operation of the system itself and its faulty output. This is like the EU Product Liability Directive 2024/2853, which makes AI subject to the Product Liability Directive, so it is liable for no reason. By globalising this standard through the IALP, we avoid what has been dubbed Liability Havens, in which corporations transport their headquarters to more obscure jurisdictions with weaker law in tort to avoid liability for the harm their models cause in foreign territories (Bas, 2026).

To avoid regulatory fragmentation and Regulatory Arbitrage, the IALP proposes a system of Mutual Recognition of Conformity. This system makes use of the logic of the CE Mark found in Article 48 in the EU AI Act. Under this pillar, the IAIA would draw up a suite of harmonised international standards (with reference to ISO / IEC 42001), which all signatories would agree to recognise (ISO/IEC 42001:2023).

A provider which is certified to a Conformity Certificate by a recognised body (such as an EU Notified Body) would see their certification passported through the IAIA to be deployed globally. In return for this access to the market, the provider agrees to have its liability subject to the IALP's rules for liability. This creates a Global Regulatory Floor: a corporation cannot declare its model safe enough for the European market, not subject to the same standards, when deployed in a developing nation. The IALP ensures that the certification of safety is to be certified to all mankind, not only to the wealthy.

The most important innovation for the Global South is the creation of the Victim Compensation Fund (VCF). History has revealed that even under strict liability, victims in poor countries often have a difficult battle ahead enforcing judgments on multi-billion-dollar foreign companies with no assets in the place where the judgment was obtained (de Graaf, 2024).

The VCF would be funded by a mandatory Digital Liability Levy - a small percentage (e.g. 0.1%) of global revenue generated by high-risk AI models. Modelling on the International Oil Pollution Compensation (IOPC) Funds, this fund would offer immediate redress to victims in

jurisdictions with weak domestic courts or where it is too difficult to establish a causal chain of an AI harm through a tort suit. This fund serves to fulfil the UN's objective of Inclusive Data Governance by ensuring the profits of AI innovation are used to curb specific risks that innovation imposes on the world's most vulnerable populations (IOPC Fund Convention, 1992).

By incorporating these three pillars in the framework of the IAIA, the IALP converts the EU's regional Gold Standard into universals. It goes beyond the soft law ethics of the early 2020s and gives the hard law enforcement of the late 2020s. For the non-state AI provider, the protocol provides the benefit of Legal Certainty; for the Global South, it provides the benefit of Protection and Redress; and for the international community, it provides the benefit of a Sustainable Social Contract for the digital age.

7. Global South & The Brussels Effect

The spread of the EU's regulatory standards across the world has often been hailed as the triumph of trustworthy AI, known as the Brussels Effect. However, from the perspective of the Global South, this phenomenon seems to be more subject to critical interrogation. Scholars and policymakers in developing countries are increasingly asking why the imposition of European High-Risk classifications and conformity assessments is a new type of Digital Colonialism (Bradford, 2020). By setting the Gold Standard in Brussels, the EU selects for the African, Asian and Latin American nations between expensive compliance, which would drain their local innovative capacity, or exclusion from the European digital market. This Regulatory Export often ignores the socio-economic realities of the Global South, where the main AI risks can be less about high-end surveillance, and more about lack of basic digital infrastructure and about abuse of the localised datasets (Anjos, 2023).

The way out of this EU-centric impasse is multilateralization of the European model, via the UN Global Digital Compact (GDC). Rather than seeing the Brussels Effect as a unilateral mandate, the international community should take advantage of the 2025 UN GDC framework to amend these regional standards into a collaborative Global Shield. Under the GDC, the Global South gets a formality at the Table of technical standardisation. This transition is to ensure that the International AI Liability Protocol (IALP) is not some kind of European transplant, but a multilaterally negotiated treaty that includes Data Sovereignty as a core principle (Lindseth, 2022).

By combining technical robustness in the EU with the media on engaging people in the UN, the IALP protects the Global South from merely serving as a pool of data and illustration for algorithms designed in the North. It seeks to change the power imbalance from that of passive adoption to that of active participation, to ensure that the burden of liability lies with the non-state provider and not the host state. Ultimately, this multilateral approach is to ensure that AI regulation is a tool for global equity rather than global division (North-South exclusion).

8. Conclusion

The European Union has clearly established the technical how of AI accountability in terms of the normative synergy between the AI Act (2024/1689) and the Revised Product Liability Directive (2024/2853). By pioneering the Presumption of Defectiveness and strict liability for systemic risks, the EU has provided a working blueprint for civil redress within the algorithmic centering on age. However, whilst the Brussels Effect has been able to establish the regulatory benchmark, it falls into a geographically siloed solution. The United Nations now needs to resolve the problem by operationalising the 2025 Global Digital Compact (GDC) into a binding International AI Liability Protocol (IALP). The future of global digital justice is based on this transformation from regional standards to universal law. Without a UN-anchored protocol through which to multilateralise the EU's liability mechanics, international legal order runs the risk of a Liability Divide for the Spectacle that will likely never end. In this kind of chopped-up, non-state-based world, human rights would be on

European soil, and so the rest of the world and the Global South would be the open laboratory without requiring any non-state-based ethical accountability on AI-harm. To avoid the risk of a new generation of digital colonialism, the international community must universalise the digital social contract, which will ensure that accountability follows the algorithm across all borders.

Author Declaration

- State no conflicts of interest

References

Anjos, L. (2023). Under the shadow of the Brussels effect: a critical assessment of the regulation of new technologies in the Global South. *Available at SSRN 4872379*.

Baş Süzel, E. (2026). The Concept of Damage under the 2024/2853 Product Liability Directive–A Comparison with Turkish Law. *Journal of European Tort Law*, *17*(1), 38-70.

Bauer, M., & Pandya, D. (2024). *EU autonomy, the Brussels Effect, and the rise of global economic protectionism* (No. 01/2024). ECIPE Occasional Paper.

Bradford, A. (2020). *The Brussels effect: How the European Union rules the world*. Oxford University Press.

Chaudhuri, N. (2021). Artificial Intelligence and International Law: Towards a New Accountability Framework. *De Lege Ferenda*, *4*, 1.

Council of Europe. (2024). *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law* (CETS No. 225). https://rm.coe.int/1680afae3c

Council of Europe. (2024). *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law* (CETS No. 225).[6]

Danila, G. (2025). Selected Judgements of the Court of Justice of the European Union in the First Semester of 2025. *Jurnalul Baroului Cluj*, 63.

Dawson, M. (2023). The accountability of non-governmental actors in the digital sphere: A theoretical framework. *European Law Journal*, *29*(1-2), 78-90.

de Graaf, T. (2024). Liability for artificial intelligence in EU Law. In *Research Handbook in Data Science and Law* (pp. 117-136). Edward Elgar Publishing.

Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC. (2024). *Official Journal of the European Union*, L. http://data.europa.eu/eli/dir/2024/2853/oj

Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC.[1] (2024). *Official Journal of the European Union*, L, 2024/2853.

Dun & Bradstreet Austria GmbH v Österreichische Datenschutzbehörde, Case C-203/22, ECLI:EU:C:2025:156 (2025).

Erman, E., & Furendal, M. (2025). The democratic role of non-state actors in the global governance of artificial intelligence. *Critical Review of International Social and Political Philosophy*, 1-26.

European AI Office. (2025). *Code of practice for providers of general-purpose artificial intelligence (GPAI) models*. European Commission.

European AI Office. (2025). *Code of practice for providers of general-purpose artificial intelligence (GPAI) models*. European Commission.

European Convention on Human Rights, opened for signature Nov. 4, 1950, 213 U.N.T.S. 221.

International Convention on the Establishment of an International Fund for Compensation for Oil Pollution Damage (IOPC Fund Convention). (1992). 1911 U.N.T.S. 3.

International Organisation for Standardization & International Electrotechnical Commission. (2023). *Information technology — Artificial intelligence — Management system* (ISO/IEC Standard No. 42001:2023). https://www.iso.org/standard/81230.html

Ishkhanyan, A. (2025). Governing AI across borders: corporate power, state sovereignty and global regulation. *Digital Policy, Regulation and Governance*.

Leonetti, M., & Pecoraro, V. (2025, September). Governing Artificial Intelligence in the European Union: Risk, Ethics, and the Architecture of the AI Act. In *International Conference on Information Technology for Social Good* (pp. 213-216).

Lindseth, P. L. (2022). The Brussels Effect: How the European Union rules the world.

Malacka, M. (2024). AI Legislation, Private International Law and the Protection of Human Rights in the European Union. *European Studies–The Review of European Law, Economics and Politics*, *11*(1), 122-151.

Maslej, N., Fattorini, L., Perrault, R., Gil, Y., Parli, V., Kariuki, N., ... & Oak, S. (2025). Artificial intelligence index report 2025. *arXiv preprint arXiv:2504.07139*.

Niazi, Maral. "How Do Current AI Regulations Shape the Global Governance Framework?." (2025).

Ponce, A. (2025). The Right to Meaningful Explanation in Algorithmic Management: Commentary on the CJEU's judgment in Dun & Bradstreet Austria, Case C-203/22.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). (2016). *Official Journal of the European Union*, L 119/1. http://data.europa.eu/eli/reg/2016/679/oj

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). (2016). *Official Journal of the European Union*, L 119/1. http://data.europa.eu/eli/reg/2016/679/oj

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).[3] (2016). *Official Journal of the European Union*, L 119/1.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).[2] (2024). *Official Journal of the European Union*, L, 2024/1689.

Revolidis, I. (2024). Regulating General Purpose Artificial Intelligence (GPAI) within the EU AI Act: Challenges and Considerations. *Available at SSRN 5122935*.

RÖTTGER, P., HOVY, D., NOZZA, D., & VANSCHOREN, J. (2025). General-Purpose AI Model Reach as a Criterion for Systemic Risk.

SCHUFA Holding (Scoring), Case C-634/21, ECLI:EU:C:2023:957 (2023).

UNESCO. (2021). *Recommendation on the Ethics of Artificial Intelligence*.

United Nations. (1945). *Charter of the United Nations and Statute of the International Court of Justice*. https://www.un.org/en/about-us/un-charter/full-text

United Nations. (1945). *Charter of the United Nations and Statute of the International Court of Justice*. https://www.un.org/en/about-us/un-charter/full-text

United Nations. (2024). *Global Digital Compact: An open, free and secure digital future for all*. https://www.un.org/techenvoy/global-digital-compact

United Nations. (2024). *Global Digital Compact: An open, free and secure digital future for all*. https://www.un.org/techenvoy/global-digital-compact

United Nations. (2024). *Global Digital Compact: An Open, Free and Secure Digital Future for All*. https://www.un.org/techenvoy/global-digital-compact

Yilma, K. (2025). The Global Governance of AI: The Role of the United Nations.