Artificial Intelligence and Corporate Liability Towards a New Legal-Ethical Contract in the Dynamics of Emerging Global Human Rights Convergences

Associate professor **Cristina Elena POPA TACHE**[1]
Associate professor **Elise Nicoleta VÂLCU**[2]

Abstract

Artificial intelligence is remapping the foundations of the interaction between technology, corporations and human rights, through a profound rethinking of the ethical-legal contract that links them. The article is based on an inter-, multi-, even transdisciplinary and critical reading of the transformations brought by AI in the sphere of corporate responsibility, starting from the premises of a governance that integrates moral lucidity and normative rigour. Instead of fragmented or purely reactive regulation, a shared collective responsibility is taking shape. Algorithmic technologies, while appearing to be neutral instruments, must be treated as expressions of institutional wills that effectively shape social reality. In this system, due diligence becomes a practice of continual vigilance, and legal liability extends to hitherto ignored areas, such as system design, data selection and the impact on individual autonomy. A vision in which corporations actively contribute to upholding human dignity, ecological balance and democratic pluralism by assuming a moral contract that precedes and underpins positive regulation is brought to the fore. The approach is academic and critical, linking legal doctrine, regulatory analysis, relevant case law and technological impact. The conclusions emphasise the emergence of a new legal-ethical system in which companies developing or using AI are legally and morally bound to prevent and remedy adverse effects on human rights.

Keywords: *artificial intelligence, corporate accountability, human rights, legal-ethical contracts, digital governance, global justice, due diligence, anticipatory liability, the United Nations Treaty on Business and Human Rights.*

JEL Classification: *K24, K33, K38*

DOI: 10.62768/TBJ/2025/15/2/04

Please cite this article as:	**Article History**
Popa Tache, Cristina Elena & Elise Nicoleta Vâlcu, 'Artificial Intelligence and Corporate Liability Towards a New Legal-Ethical Contract in the Dynamics of Emerging Global Human Rights Convergences', *Juridical Tribune – Review of Comparative and International Law* 15, no. 2 (June 2025): 281-305.	Received: 20 March 2025 Revised: 18 April 2025 Accepted: 27 May 2025

[1] Cristina Elena Popa Tache – Faculty of Psychology, Behavioral Sciences and Law, „Andrei Șaguna" University of Constanta, Romania; Chair for the International Institute for the Analysis of Legal and Administrative Mutations; active research member of CIRET Paris; Co-Convenor for ESIL IG International Business and Human Rights, cristinapopatache@gmail.com. ORCID: 0000-0003-1508-7658.

[2] Elise Nicoleta Vâlcu – Faculty of Economic Sciences and Law, within the National University of Science and Technology Politehnica Bucharest, Pitești University Centre, Romania; arbitrator at the Court of Arbitration attached to the Chamber of Commerce, Industry and Agriculture Argeș, Romania; lawyer at the Argeș Bar, Romania, elisevalcu@yahoo.com. ORCID: 0000-0001-6255-164X.

1. Methods

A complex set of methodological tools, based on formal logic, legal dialectics and a synergetic interdisciplinary approach, was used to elaborate this study, which allowed a rigorous articulation of concepts and a critical evaluation of the normative framework applicable to artificial intelligence systems, either autonomous or integrated into products.

The proposed analysis, as well as the selected thematic areas, stands out for their scientific relevance and originality, contributing to a deeper understanding of the liability typologies associated with new technologies. In particular, the research responds to the challenges generated by the diversity of risks induced by the characteristics of emerging AI systems.

The arguments developed in this paper are based on the premise that accelerated digitisation and the proliferation of new technological systems have radically transformed (and continue to transform) the business environment and commercial practices. In turn, these transformations have accentuated consumer vulnerabilities, notably by creating new forms of 'information asymmetry'. The study argues the need for a harmonised legal framework, consistent with national liability rules and capable of ensuring legal certainty both within the EU and internationally.

2. Introduction

Recent years have been influenced by the rise of artificial intelligence (AI) technologies that are either autonomous or integrated in various ways into digital products, and the issue of legal liability for damages generated by these systems is therefore gaining significant urgency, leading to the need to rethink the traditional vision of legal liability. Businesses that develop and implement AI face high human rights risks, from algorithmic discrimination and privacy violations to physical harm caused by autonomous vehicles. Traditional international legal instruments have been slow to adapt and have lagged behind these technological developments, leaving a scission in the governance of corporate responsibility. In the absence of binding international rules, corporate liability for AI-related human rights abuses regulated by national laws is often insufficient or difficult to enforce in cross-border situations. Relevant international initiatives exist, one of them being the Draft UN Treaty on Business and Human Rights[3] (negotiated in the UN Human Rights Council through the

[3] United Nations Human Rights Council. *Updated Draft Legally Binding Instrument to Regulate, in International Human Rights Law, the Activities of Transnational Corporations and Other Business Enterprises*. OEIGWG, 9th Session, July 2023. https://www.ohchr.org/sites/default/files/documents/hrbodies/hrcouncil/igwg-transcorp/session9/igwg-9th-updated-draft-lbi-clean.pdf. Also see Chair-Rapporteur of the Open-ended Intergovernmental Working Group (OEIGWG). *Updated February 2025 Roadmap and Methodology for the Implementation of HRC Decision 56/116*. February 2025. https://media.business-humanrights.org/media/documents/Updated_Feb_2025-Roadmap_and_Methodology_IGWG_treaty.pdf. For new details see Mingrone, Francesca and Suárez-Franco, Ana María, 'Grounding the new legally binding instrument on transnational corporations on the right to a healthy environment', *Third World Resurgence*, no. 362 (March 2025), Accessed May 5, 2025, https://twn.my/title2/resurgence/2025/362/

OEIGWG[4]), which, if adopted, would be a welcome legal instrument to strengthen the liability regime applicable to technology companies at the global level.

For these reasons, this article discusses the relevance of this draft treaty to the legal accountability of AI systems, highlighting corporate due diligence obligations, the links to fundamental human rights principles, and transnational issues of jurisdiction and access to justice in the global digital economy. Notwithstanding its general orientation, the Draft UN Treaty on Business and Human Rights has a particularised normative vocation, primarily targeting transnational corporations, with a focus on their accountability in global value chains. While the current wording allows for a broad application, the implicit inclusion of other forms of enterprise is conditional on the degree of involvement in economic activities with a cross-border effect and the capacity to cause, directly or indirectly, significant damage to fundamental rights. Therefore, Big Tech companies, by the magnitude of the digital infrastructure and the transnational data flows they control, fall comfortably within the regulatory scope of the Directive. In contrast, for medium-sized or local tech players, the regime proposed by the Treaty would be perceived as an aspirational legal regime rather than a legal constraint in its own right.

It is therefore necessary to clearly delimit the international legal instruments that address technology firms according to their nature and level of operationalisation. The UN Guiding Principles on Business and Human Rights (UNGPs)[5] and the OECD Guidelines for Multinational Enterprises[6] function as soft law reference models, through functional due diligence and human rights risk prevention standards, which become applicable not only directly, but also through contractual mechanisms imposed by partners or investors, especially in platform ecosystems, where small and medium-sized firms become part of multinational digital structures. Alongside these, in the European regulatory space, legislative sets such as the GDPR[7], the Digital Services

cover03.htm; and Vecellio Segate, Riccardo. 2021. "The First Binding Treaty on Business and Human Rights: A Deconstruction of the EU's Negotiating Experience along the Lines of Institutional Incoherence and Legal Theories." *The International Journal of Human Rights* 26 (1): 122–59. doi: 10.1080/13642987.2021.1895767.

[4] OEIGWG stands for an Open-Ended Intergovernmental Working Group, a body of the UN Human Rights Council, created by UN Human Rights Council Resolution 26/9 (2014) with the aim of elaborating a *legally binding* international instrument on the activities of transnational corporations and other business enterprises in relation to human rights.

[5] United Nations Human Rights Council, *Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework*, UN Doc. A/HRC/17/31 (2011).

[6] Organisation for Economic Co-operation and Development (OECD), *OECD Guidelines for Multinational Enterprises*, 2011 Edition (Paris: OECD Publishing, 2011). https://www.ohchr.org/sites/default/files/Documents/Issues/Business/A-HRC-17-31_AEV.pdf.

[7] European Union, 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 – *GDPR*), Official Journal of the European Union, L 119/1, 4 May 2016. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.

Act[8], the Digital Markets Act[9] or the AI Act[10] enshrine a functional legal treatment, in which the distinction between the economic dimension and the impact on fundamental rights is dissolved in favour of an integrated technical-legal regime[11]. Legal liability becomes algorithmic and regulation is built around the automated processes and digital infrastructure that a corporation, as an economic actor, maintains.

2.1. Between Past and Future

Thus, for a large proportion of tech businesses, especially those that do not fall under the classic definition of transnational enterprise, traditional treaties are giving way to emerging legal constructs, where the convergence of compliance regimes, digital governance and the protection of fundamental rights are becoming the centrepiece of the normative future. The UN Treaty, while fundamental in shaping the global corporate accountability architecture, remains relevant in particular as a benchmark and activation tool for further legal developments, notably on extraterritoriality and access to justice in collective or cross-border cases. The meteoric development of artificial intelligence technologies over the last decade has brought economic and social benefits, but also significant risks for human rights and society. AI can optimise processes and solve difficult problems, but if legal accountability mechanisms do not evolve with technological progress, the use of AI can lead to serious violations of fundamental rights[12]. This is particularly important because AI systems are largely developed and controlled by private entities, and corporate self-regulation has proven insufficient – 'AI is simply too powerful, and the consequences for rights are too severe, to allow companies to self-regulate'[13].

[8] European Union, Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act), Official Journal of the European Union, L 277/1, 27 October 2022.https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng.

[9] European Union, Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on Contestable and Fair Markets in the Digital Sector (Digital Markets Act), Official Journal of the European Union, L 265/1, 12 October 2022, https://eur-lex.europa.eu/eli/reg/2022/1925 /oj/eng.

[10] Regulation (EU) 2024/1689 of 13 June 2024, Laying Down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). Official Journal of the European Union L 2024/1689, 12 July 2024, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689.

[11] See for an applied comparative view Martin, Baily. "Privacy in a Programmed Platform: How the General Data Protection Regulation Applies to the Metaverse." *Harvard Journal of Law & Technology* 36, no. 1 (Fall 2022): 235–261. Accessed June 6, 2025. https://jolt.law.harvard.edu/assets/articlePDFs/v36/Martin-Privacy-in-a-Programmed-Platform.pdf.

[12] Liebholz, Alina, 'Commentary: Who is Liable if AI Violates Your Human Rights?,' *Impakter*, reprinted from *Business & Human Rights Resource Centre*, 28 May 2023, Accessed May 5, 2025, https://www.business-humanrights.org/en/latest-news/company-liability-for-human-rights-violations-caused-by-ai/.

[13] Bacciarelli, Anna and Aufiero, Paul, 'Pandora's Box: Generative AI Companies, ChatGPT, and Human Rights,' *Human Rights Watch*, 3 May 2023, Accessed May 5, 2025, https://www.hrw.org/news/2023/05/03/pandoras-box-generative-ai-companies-chatgpt-and-human-rights.

At the international level, until recently there has been no unitary or globally agreed normative regime for the relationship between AI and human rights, but companies nevertheless have a responsibility to respect human rights under international law (notably through instruments such as the UN Guiding Principles on Business and Human Rights from 2011). We are currently observing a global effervescence in the development of a new ethical-legal contract to govern corporate responsibility in the digital age. This 'contract' is built from both hard law norms such as treaties, regulations, binding directives, and soft law standards, such as voluntary principles and guidelines, along with heightened ethical expectations from civil society.[14]

This paper starts from the premise that the technological transformations imposed by AI require a reconceptualisation of corporate responsibility, moving beyond the traditional boundaries of territorial and sectoral corporate responsibility. We will analyse how global human rights initiatives (such as the forthcoming UN Treaty on Business and Human Rights) and the new European legislative framework (including the AI Act and related legislation) are reshaping companies' obligations, creating the premises for a new ethical-legal contract[15]. Through an integrated analysis of legal doctrine, recent regulatory provisions, recent case law and technological impact considerations, the paper highlights both the advances and gaps in ensuring corporate accountability in the AI era. With this in mind, the conclusions will take into account the evolutionary directions of corporate accountability and the need to align it with the ethical and legal demands of contemporary society.

3. The Triangular Conceptual Configuration of AI, Corporate Accountability and Human Rights

The concept of the legal-ethical contract is not recognised as a standardised legal category in classical positive law, but it is used in interdisciplinary contexts, notably in applied ethics, political philosophy, and sometimes in international law or constitutional doctrine**.** If we were to define it, we would say that it is a conceptual or normative agreement, formal or informal, by which the parties assume mutual obligations combining legal requirements (normative, sanctionable, institutionalised) with ethical ones (moral values, responsibility towards the other, common good), aiming at maintaining a social, inter-human or institutional order that is just, sustainable and responsible. It is a bridging concept between what should be (ethics) and what is regulated (law).

Corporate responsibility towards human rights is a concept crystallised over the

[14] Yazici, Tuana "Toward a Global Standard for Ethical AI Regulation: Addressing Gaps in AI-Driven Biometric and High-Resolution Satellite Imaging in the EU AI Act." *Law, Innovation and Technology* 17 (1) 2025.: 366–394. doi:10.1080/17579961.2025.2470589, Accessed May 5, 2025, https://www.tandfonline.com/doi/full/10.1080/17579961.2025.2470589.

[15] Piasecki, Stanislaw, and Natali Helberger, 'A Nightmare to Control: Legal and Organisational Challenges around the Procurement of Journalistic AI from External Technology Providers.' *The Information Society* 41 (3) 2025: 173–194. doi:10.1080/01972243.2025.2473398, Accessed May 2, 2025, https://www.tandfonline.com/doi/full/10.1080/01972243.2025.2473398.

last decade through instruments such as the UN's Guiding Principles on Business and Human Rights (UNGPs). Adopted in 2011 as *soft law*, the UNGPs represented a turning point and provided, 'a critical foundation for integrating human rights into business practices and emerging regulations'[16]. According to the UN Guiding Principles, businesses have a responsibility to respect human rights, which involves due diligence to identify, prevent and mitigate risks of human rights abuses in any of their operations and supply chains. In the years since their adoption, there has been an increase in the number of companies that have adjusted their internal policies to follow the UN Guiding Principles. Over a decade on, voluntary implementation has often proved insufficient, and recent assessments show that most companies have made only marginal progress and are limited to the early stages of human rights due diligence. Thus, it is clear that voluntary measures and self-regulation alone cannot cover the protection of rights in the face of new challenges brought by technology.

Artificial intelligence amplifies these problems. AI systems, especially 'black box' (opaque) systems, can produce effects that are unpredictable or difficult to attribute to a direct human cause. As an example, machine learning algorithms can generate discrimination in employment or access to financial services without the discriminatory intent being human, raising the question of who is responsible for these rights violations (the developer company, the user, the software manufacturer, etc.). The absence of legislative adaptations puts victims of AI harms at risk of effective access to remedies, and companies may evade liability in some cases, as it has been observed that the proposed new EU Directives on AI liability, while creating a uniform framework, leave potential liability gaps for harms caused by complex black-box systems, such as some AI in the medical field[17]. Patients harmed by opaque algorithmic decisions face difficulties in successfully holding manufacturers or healthcare providers liable under the current strict or fault-based liability regimes. Uncertainty is therefore generated, highlighting the need to update classical legal doctrines of liability to accommodate technological reality.

3.1. Towards New Regulations

At the same time, at the international level, there has been a growing realisation that the lack of a binding global legal regime allows multinational companies to avoid liability through jurisdictional arbitration[18]. In response, states have initiated global

[16] Muñoz Quick, Paloma, 'Leveling the Global Playing Field: A Binding Treaty on Business and Human Rights,' *BSR – Business for Social Responsibility*, 25 January 2024, Accessed May 9, 2025, https://www.bsr.org/en/blog/leveling-the-global-playing-field-a-binding-treaty-on-business-and-human-rights. For a comparison see Nina M Hart, Christopher A Casey, Transatlantic leadership in an era of human rights-based export controls, *Journal of International Economic Law*, Volume 27, Issue 1, March 2024, Pages 130–146, https://doi.org/10.1093/jiel/jgae005.

[17] Duffourc, Mindy Nunez Mindy and Gerke, Sara, 'The Proposed EU Directives for AI Liability Leave Worrying Gaps Likely to Impact Medical AI,' *npj Digital Medicine* 6, Article No. 77 (April 2023), Accessed May 9, 2025, https://www.nature.com/articles/s41746-023-00823-w.

[18] Mahmoud, Amira, 'Bridging Global and Regional Perspectives in ISDS Reform: Regional Mechanisms and Legal Empowerment for the Middle East and Africa Regions', International Investment Law Journal 5,

human rights projects aimed at discouraging governance gaps and imposing common standards. Efforts to draft a legally binding UN Treaty on Business and Human Rights, initiated in 2014 and still under negotiation, are eloquent. The draft seeks to compel states to develop regulations with the aim that companies respect human rights and be held accountable for violations along the global value chain. The updated version of the draft treaty (July 2023) focuses on victims' rights to remedies and requires governments to compel companies to conduct regular human rights impact assessments. Coordinated, it expands the concept of companies' legal accountability by including both the civil, criminal and administrative sides of liability for violations. The adoption of such a treaty would mark a significant leap from voluntary principles to explicit legal obligations for corporations at the transnational level, transposing the UNGPs into a binding legal regime.

But the road to a global deal is not without controversy. Civil society organisations have welcomed the initiative, but criticised some watering down in the negotiations. In this regard, the International Federation for Human Rights (FIDH) notes that the 2023 draft, while more concise, has weakened some key articles on access to justice and removed important references (e.g. environmental impact, labour rights), representing, 'a step backwards from previous versions, especially on corporate liability for violations'[19]. Even if such discussions persist, the increasingly active participation of some global actors (EU, some G7 states) in the negotiations indicates a growing realisation that voluntary measures are not sufficient and that an international legal framework is needed to hold companies accountable in the AI era. The contemporary conceptual legal regime on AI and corporate responsibility is taking shape at the confluence of *soft law* principles (such as UNGPs, OECD guidelines) and new *hard law* initiatives (proposed UN treaty, EU legislation). The following chapters of the article will delve into the components of the starting first from international normative developments (soft law vs. developing hard law), then focussing on the European legislative system, and finally examining incipient jurisprudence and technological implications in order to assess to what extent we are witnessing the birth of a new legal-ethical contract adapted to the digital age.

4. Global Initiatives and Soft Law Instruments from UN Principles to a Possible Treaty

Generically, the UN Guiding Principles on Business and Human Rights (UNGP) and the OECD Guidelines for Multinational Enterprises provide the normative foundation for expectations of responsible behavior. The UNGP, adopted in 2011 by

no. 1 (February 2025): 11–29. Also see Dimitrios Devetzis și Simos Samaras, 'E-Commerce Platforms and Liability in the AI Era', *International Investment Law Journal* 4, No. 1 (februarie 2024): 19–28, https://journals.indexcopernicus.com/api/file/viewByFileId/2081836.

[19] International Federation for Human Rights (FIDH). 'United Nations Binding Treaty on Business and Human Rights: FIDH's Position Ahead of the 10th Negotiation Session.' *FIDH*, July 2023, Accessed May 2, 2025, https://www.fidh.org/en/issues/business-human-rights-environment/business-and-human-rights/un-binding-treaty-position-2023.

the UN Human Rights Council, enshrine the three pillars, namely the obligation of states to protect human rights, the responsibility of corporations to respect these rights, and the need for victims to have access to remedies. The UNGPs, adopted in 2011 by the UN Human Rights Council, enshrines the three pillars, namely the obligation of states to protect human rights, the responsibility of corporations to respect these rights, and the need for access to remedies for victims. Although they are soft law instruments, the UNGPs have strongly influenced the development of subsequent national and regional legislation, serving as a 'critical foundation' for integrating human rights concerns into emerging regulations[20]. One reflection of the UNGPs in regulation is even the European Union through the forthcoming Corporate Sustainability Due Diligence Directive (CSDDD) provides for human rights and environmental due diligence obligations, being explicitly inspired by the UNGPs. Furthermore, the EU's Digital Services Act (DSA) refers in its preamble to the UNGPs and borrows elements of their logic so that the DSA requires large platforms to conduct risk assessments of recommendation systems and due diligence measures, evoking the due diligence structure of the UNGPs.[21]

The OECD Guidelines for Multinational Enterprises (originally from 1976, updated periodically) were themselves updated in 2023, precisely to reflect new developments, including digital ones. The OECD added explicit recommendations on the impact of technology and AI on human rights and the environment. In addition, in May 2024, the OECD revised its Principles on AI (originally adopted in 2019), emphasising responsible business conduct throughout the lifecycle of AI systems, in line with the updated OECD Guidelines[22]. Cooperation between AI developers, suppliers and users in the value chain is encouraged so that AI is developed and deployed *with respect for human rights*. Even if these tools remain formally voluntary, they influence societal and normative expectations, as can be seen from the fact that OECD Member States are required to set up national contact points where complaints can be lodged for non-compliance with the Guidelines, generating a quasi-jurisdictional accountability mechanism. An increasing number of jurisdictions (the EU, US, Canada, Japan, etc.) are adopting laws that transform elements of these voluntary standards into legal obligations, in particular in the area of supply chain due diligence (e.g. legislation against forced labour and abuses in global supply chains).[23]

The endeavour to create a legally binding treaty on business and human rights is

[20] Muñoz Quick, Paloma, 'Leveling the Global Playing Field: A Binding Treaty on Business and Human Rights,' *BSR – Business for Social Responsibility*, 25 January 2024, Accessed May 9, 2025, https://www.bsr.org/en/blog/leveling-the-global-playing-field-a-binding-treaty-on-business-and-human-rights.

[21] Ebert, Isabel. *Fostering Business Respect for Human Rights in AI Governance and Beyond: A Compass for Policymakers to Align Tech Regulation with the UNGPs*. Carr Centre Discussion Paper, Issue 2024-05. Harvard Kennedy School, Harvard University, April 18, 2024, Accessed May 5, 2025, https://www.hks.harvard.edu/sites/default/files/2024-04/24_Ebert_TechFellowPaper.pdf.

[22] Cooley L. L P. 'OECD Guidelines on Responsible Business Conduct: Key Considerations for Multinational Enterprises.' *Cooley*, May 31, 2024, Accessed May 9, 2025, https://www.cooley.com/news/insight/2024/2024-05-31-oecd-guidelines-on-responsible-business-conduct-key-considerations-for-multinational-enterprises.

[23] Ibid.

the next step in consolidating, as far as possible a unitary global legal regime. As we have shown, a UN Intergovernmental Working Group has been negotiating a draft treaty since 2014 that, if adopted, would require signatory states to enact domestic mechanisms to hold companies accountable for human rights violations. The latest draft version available at the time of writing provides, among other things, that states must regulate the civil, criminal and administrative liability of companies for serious human rights violations, as well as the obligation to conduct human rights impact assessments and to make these assessments public on a regular basis. The stated aim is 'levelling the playing field' so that companies already implementing high standards (e.g. some European multinationals) are not put at a competitive disadvantage compared to those operating in jurisdictions with lax regulations[24]. The Treaty would thus address the root causes of abuses (global governance loopholes) that allow some actors to avoid accountability by exploiting differences between national systems.

On the other hand, the negotiations also highlight geopolitical tensions and diverging visions. Some countries (China, Russia, South Africa) are in favour of limiting the treaty to transnational corporations, while others (the EU, US, Latin American countries) want it to apply to all companies, regardless of size or transnational character. There is also pressure for the explicit inclusion in the text of issues such as environmental protection, conflict zones, children's rights and the rights of vulnerable groups. The outcome of these negotiations will directly influence the global legal-ethical regime in which AI is developed and used, in that an ambitious treaty could establish Technological Due Diligence, i.e. the assessment and prevention of the human rights impacts of algorithms, digital surveillance, etc., as a universal standard. Already parallel initiatives, such as the G7 Hiroshima Process (2023), have emphasised the need to integrate respect for human rights into AI governance by developing codes of conduct for AI developers based on the UNGPs and OECD guidelines. As an intermediate summary, it can be said that *soft law* instruments such as the UNGPs and OECD guidelines have paved the way for the recognition of corporate responsibility for human rights, including in the digital context. But the transition to *hard law*, either through a future UN treaty or through regional laws with extraterritorial vocation, is important for the effective fulfilment of these responsibilities in the AI era. Further on, we turn our attention to the European Union, which in particular has become a normative laboratory for new rules on AI and corporate responsibility.

4.1. The EU Regulatory System, Product Liability and Artificial Intelligence

The European Union has reacted swiftly to the challenges posed by AI, coming up with a coherent legislative package both to regulate the use of AI (to prevent abuses and risks) and to adapt civil liability regimes (so that victims of AI injuries can get

[24] Office of the United Nations High Commissioner for Human Rights (OHCHR), *Updated Draft Legally Binding Instrument (Clean Version) to Regulate, in International Human Rights Law, the Activities of Transnational Corporations and Other Business Enterprises*, OEIGWG, 9th Session, July 2023, Accessed May 2, 2025, https://www.ohchr.org/sites/default/files/documents/hrbodies/hrcouncil/igwg-transcorp/session9/igwg-9th-updated-draft-lbi-clean.pdf.

compensation). The package mainly includes Regulation (EU) 2024/1689 (known as the *Artificial Intelligence Act* or AI Act), the new Product Liability Directive (EU) 2024/2853 (which updates the strict liability regime, taking into account digital and AI products) and a forthcoming AI Civil Liability Directive (currently at the proposal stage, aimed at adapting the rules on tort liability to the specificities of AI). Complementary to this, the EU already has digital governance instruments, such as the General Data Protection Regulation (GDPR) and the Digital Services Act (DSA), which, although not exclusively aimed at AI, impose obligations that strongly influence the responsibility of companies in the digital environment. We will analyse these components in turn.

4.1.1. New Directive (EU) 2024/2853 on Defective Products in the Digital Age

The classic EU product liability regime (established by Directive 85/374/EEC) was centred on tangible goods and did not anticipate where software or algorithms would cause damage. In October 2024, the EU adopted a new Product Liability Directive (2024/2853), which fundamentally overhauls this legislation to adapt it to the digital age[25]. The new Directive significantly expands the notion of *product* and thus the area of no-fault liability of producers in an innovative way, covering digital products, including software and artificial intelligence systems, as well as digital services embedded in a product[26]. In other words, an AI algorithm or a software update that contributes to the functioning of a device can be considered part of the product, and its defects are thus to engage the liability of the manufacturer. The Directive explicitly states that where a product has integrated digital components (software, AI), these components are subject to the *no-fault* liability regime. In addition to extending the scope of the application, the Directive introduces other changes aimed at facilitating the compensation of victims in problematic situations typical of the digital age. Firstly, it requires authorities and courts to take into account cybersecurity requirements when assessing a possible product defect. So, if a product (e.g. an AI-enabled IoT device) does not comply with *cybersecurity* standards and is therefore vulnerable to attacks that cause harm, that lack of security can be treated as a product *defect.* In fact, it is a direct response to the growing problem of cyber-attacks and security breaches that can cause harm to consumers. Secondly, the new directive broadens the scope of potentially liable parties by making fulfilment service providers and, in certain cases, operators of online platforms through which products reach consumers, liable in addition to manufacturers and importers. Marketplace-type situations are targeted, such as if faulty products from outside the EU are sold on an online platform and the manufacturer cannot be identified

[25] European Parliament and Council of the European Union. *Directive (EU) 2024/2853 of 23 October 2024 on Liability for Defective Products and Repealing Council Directive 85/374/EEC.* Official Journal of the European Union L 2853, 18 November 2024, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024L2853.

[26] Latham & Watkins L. L P. *A new EU Product Liability Directive Comes Into Force*. Client Alert No. 3319. December 23, 2024, Accessed May 5, 2025, https://www.lw.com/en/offices/ admin/upload/SiteAttachments/New-EU-Product-Liability-Directive-Comes-Into-Force.pdf.

or held liable, the platform itself could be held liable.

Last but not least, the Directive contains procedural provisions that lower the burden of proof in favour of the plaintiff and facilitate access to evidence (possibility for the court to compel the provider to disclose algorithm information or performance data), introduce legal *presumptions* under certain conditions so that the victim is not asked to prove the impossible in proving exactly how an algorithm caused the damage. Overall, the new Directive 2024/2853 configures a 'plaintiff-friendly' strict liability regime, implicitly recognising that AI and digital products can cause harm in the same way as traditional products and that evidentiary hurdles (technical complexity, opacity) need to be compensated for by legal adjustments. Member States have until the end of 2026 to transpose these provisions, marking the deadline by which companies must prepare for stricter liability standards in the EU.

4.1.2 Regulation (EU) 2024/1689 (AI Act) – The First Comprehensive Legal Framework for AI

Concurrently with the tort reform, the EU designed a regulation dedicated to AI governance, the *Artificial Intelligence Act,* which was formally adopted in June 2024 (Regulation 2024/1689) and entered into force on 1 August 2024[27]. The AI Act is the world's first comprehensive regulation focused exclusively on artificial intelligence, aiming both to ensure security and respect for fundamental rights and to incentivise responsible innovation. Its distinctive feature lies in its risk-based approach, whereby the Regulation categorises AI applications according to the level of risk they pose to human rights and safety and imposes graduated obligations in proportion to the risk identified.

Thus, certain uses of AI are labelled as unacceptable risks and explicitly prohibited, such as real-time biometric surveillance systems in the public space or social scores generated by governments or companies (assessing citizens based on behaviour, similar to the concept of social scoring). The aim of these bands is to protect fundamental values such as human dignity, privacy and non-discrimination in situations where the use of AI would be considered inherently contrary to these values (e.g. mass biometric surveillance violates the right to privacy and may discourage freedom of assembly).

The central category covered by the AI Act is high-risk AI systems. This includes uses of AI in sensitive areas, such as product safety (e.g. safety systems in critical infrastructure or autonomous vehicles), education and employment (e.g. recruitment or assessment algorithms), essential services (credit scoring, assessment systems for

[27] European Parliament and Council of the European Union. *Regulation (EU) 2024/1689 of 13 June 2024, Laying Down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)*. Official Journal of the European Union L 2024/1689, 12 July 2024. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689. Also see ISACA, *Understanding the EU AI Act: Requirements and Next Steps* (Schaumburg, IL: ISACA, 18 October 2024), https://www.isaca.org/resources/white-papers/2024/understanding-the-eu-ai-act.

public benefits), law enforcement (systems that may affect rights in a police or judicial context), biometric recognition (retrospective facial identification), etc.[28] . For these systems, the Act introduces strict obligations before they are placed on the market. Obligations include implementing a risk management system and ex ante risk assessments, ensuring high quality of training data to minimise possible discriminatory results, keeping activity logs for traceability, developing detailed technical documentation to allow authorities to assess compliance, providing adequate information to the users (deployers) about the purpose and limitations of the system, ensuring adequate human supervision and achieving high standards of robustness, cybersecurity and accuracy. This set of requirements positions the AI Act at the intersection of two EU legal traditions, between product safety (akin to regulations in the technical equipment sector) and the protection of fundamental rights[29]. Basically, for a high-risk IA system, the manufacturer (supplier) has to obtain a conformity certification before placing it on the market, similar to the CE marking, demonstrating that all the above requirements are met. The Regulation also provides for market surveillance mechanisms, specifying that national authorities will monitor and may withdraw or penalise AI systems that do not comply with these obligations, and that economic operators (suppliers, distributors, users) have duties to report serious incidents and to co-operate with the authorities.

Another innovative element of the Act is the imposition of transparency requirements for certain AI systems interacting with the public. For example, if a person interacts with a chatbot or other AI agent, they must be clearly informed that the interlocutor is a machine, not a human. Similarly, AI-generated audio-visual content (so-called *deepfakes*) that may mislead the audience should be prominently labelled as synthetic. In addition, providers of generative AI models (such as GPT-4) will be required to integrate measures to ensure that generated material can be identified as such and to prevent misuse, including respecting copyright for training data.

The AI Act has been hailed as a global benchmark for regulating the technology, but it has also attracted criticism. Some experts and digital rights organisations have argued that the final version of the Act does not go far enough in protecting human rights, citing exceptions or ambiguities that could be exploited[30]. AlgorithmWatch and other groups warned that some mass surveillance practices are not fully prohibited or that the list of high-risk areas could be expanded. However, the Act remains the first instrument to explicitly place legal obligations on AI producers and users to respect

[28] Schuett, Jonas. “Risk Management in the Artificial Intelligence Act.” *European Journal of Risk Regulation* 15, no. 2 (2024): 367–85. https://doi.org/10.1017/err.2023.1.

[29] Almada, Marco, and Nicolas Petit. ‘The EU AI Act: Between the Rock of Product Safety and the Hard Place of Fundamental Rights.’ *Common Market Law Review* 62, no. 1 (2025): 85–120, Accessed May 8, 2025, https://kluwerlawonline.com/journalarticle/Common+Market+Law+Review/62.1/COLA2025004.

[30] Ness, James, ‘The EU’s AI Act Fails to Set the Gold Standard for Human Rights.’ *European Disability Forum*, April 3, 2024. Accessed May 9, 2025, https://www.edf-feph.org/publications/eus-ai-act-fails-to-set-gold-standard-for-human-rights/. Also see Tyler Markoff ‘The First of Its Kind: The EU AI Act and What It Means for the Future of AI.’ *Fordham Journal of Corporate & Financial Law*, April 23, 2024, Accessed May 9, 2025, https://news.law.fordham.edu/jcfl/2024/04/23/the-first-of-its-kind-the-eu-ai-act-and-what-it-means-for-the-future-of-ai/.

fundamental rights. Breaches of these obligations attract severe penalties – administrative fines of up to 6 per cent of a company's global turnover (similar in order of magnitude to the fines in the GDPR), which provides the necessary enforcement bite.

The Act's hybrid approach is also noteworthy, combining product law elements (technical requirements, certification) with human rights law elements (rights impact assessment, transparency, ethical prohibitions). It is also able to serve as a model for other jurisdictions or future IA treaties. However, authors such as Almada and Petit emphasise that the combination of two different legal regimes comes with different practical and conceptual confrontations, as the structural differences between product safety and human rights regimes may generate tensions that will need to be resolved in the implementation phase and through subsequent legislation.[31]

4.1.3. Proposed AI Liability Directive

As a complementary part of its regulatory package, the European Commission proposed (on 28 September 2022) a Directive adapting the rules on non-contractual civil liability to artificial intelligence, commonly referred to as the AI Liability Directive. The aim of this forthcoming Directive is to remove the legal obstacles that a person who has suffered an injury caused by an AI system would face when seeking compensation under tort law (tort, fault-based civil liability). Essentially, the Directive aims to harmonise certain procedural aspects at the EU level and to ensure that 'persons injured by AI systems enjoy the same level of protection as those injured by other technologies'[32]. A central element introduced by the proposal is the establishment of legal presumptions of causation. Given the opaque and complex nature of many AI systems, the victim may have major difficulties in proving a causal link between the AI defect or behaviour and the injury. Under the proposed Directive, under certain conditions (e.g. if the plaintiff can show that the operator or manufacturer of a high-risk AI system has breached a legal duty under the AI Act, such as the duty to carry out risk assessments or to provide human supervision), a causal link between that breach and the harm will be presumed[33]. In fact, this presumption is rebuttable, but is intended to shift the burden of proof to the defendant (company), which will have to prove either that it has complied with its obligations or that the harm was not caused by its system. The measure reflects explicit recognition of the unique evidentiary difficulties created by AI and the intention to prevent situations where no one can be held liable because of technological difficulties. The proposal foresees a right for plaintiffs to seek disclosure

[31] Almada, Marco and Petit, Nicolas, 'The EU AI Act: Between the rock of product safety and the hard place of fundamental rights', Common Market Law Review, 62, No. 1, (2025): 85–120, Accessed May 8, 2025, https://kluwerlawonline.com/journalarticle/Common+Market+Law+Review/62.1/COLA2025004.

[32] European Commission. 'Liability Rules for Artificial Intelligence.' Accessed May 10, 2025. https://commission.europa.eu/business-economy-euro/doing-business-eu/contract-rules/digital-contracts/liability-rules-artificial-intelligence_en.

[33] See European Commission. *Proposal for a Directive of the European Parliament and of the Council on Adapting Non-Contractual Civil Liability Rules to Artificial Intelligence (AI Liability Directive)*. COM (2022) 496 final, September 28, 2022. Accessed June 6, 2025. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0496.

of information about defendants' AI systems, with the authorisation of the court, in order to obtain evidence necessary for the case (e.g. audit logs of AI decisions, performance data, etc.). The mechanism is reminiscent of the concept of 'discovery' in Anglo-Saxon law, but adapted to the algorithmic context, inferred from the fact that without access to the internal opacity of the algorithm, the victim cannot prove fault. The Directive would thus create the framework for courts to order companies to open their AI 'black box', under commercial confidentiality controls, to allow justice to shed light. It is important to note that the AI Liability Directive does not create a substantial new liability regime, but harmonises procedures and removes obstacles in the application of existing fault-based liability regimes. It applies, complementary to the Product Defects Directive, in situations where the damage is not covered by the strict product regime (e.g. *pure economic loss* or damage caused by AI systems, which are clearly not 'products'). The proposal provides that Member States may also maintain or adopt stricter rules at the national level. Although it has a limited role, this directive will be an important piece in the puzzle of **corporate** liability for AI, in that, even in fault-based liability cases, victims are not left out of the loop because of the nature of AI.

The literature has welcomed the intention of the Directive, but has also identified potential loopholes, as a study in npj Digital Medicine (2023) notes that neither the new Product Directive nor the AI Directive fully addresses the scenario of opaque medical AI systems. Under them, a patient harmed by a decision of a black-box clinical algorithm would fall precisely in an area not firmly covered by either strict liability (if the algorithm is considered a service, not a product) or the presumptions of the AI Directive (if no specific breach of an obligation can be identified)[34]. Such observations suggest that, however advanced the legislation may be, practice and case law will have to complement and refine it, adapting to the diversity of situations on the ground.

Overall, the EU is therefore proposing a 360° regulation, whereby the AI Act sets *ex-ante* rules for development and placing on the market (prevention and compliance), while the updated Product Directive comes with strict liability for product defects/IAs causing damage, and the AI Liability Directive will facilitate fault actions when algorithms intervene. Together, these instruments shape a new legal contract between business and society in technology, where innovation is only accepted on the condition that rights are respected and liability for possible damages is accepted.

4.1.4. Other Relevant Digital Governance Elements: GDPR, DSA, DMA

In addition to specific AI-focused legislation, there are also horizontal laws in the EU which, although not exclusively related to artificial intelligence, play a very important role in empowering companies in the digital ecosystem, which we briefly touch on below.

The General Data Protection Regulation (GDPR) has been in force since 2018 and imposes stringent obligations on companies regarding the processing of personal

[34] Duffourc, Marie-Naëlle, and Gerke, Sara, 'The Proposed EU Directives for AI Liability Leave Worrying Gaps Likely to Impact Medical AI.' *NPJ Digital Medicine* 6 (2023): 77, Accessed May 9, 2025, https://doi.org/10.1038/s41746-023-00823-w.

data. As AI is often data-hungry, many systems involve collecting and analysing large volumes of personal data (from consumer preferences to facial images for biometric recognition). GDPR obliges companies to lawfulness, transparency and security of data processing and gives individuals rights (including the right not to be subject to a decision based solely on automated processing that produces significant legal effects, according to Art.22 GDPR). Failure to comply with these provisions has attracted considerable penalties, demonstrating that corporate data liability is real. A well-known case is that of ChatGPT in Italy, when, in March 2023, the Italian data protection authority (Garante per la Privacy) temporarily suspended access to ChatGPT on the grounds of GDPR violations (lack of a legal basis for the use of personal data for model training and insufficient transparency)[35]. Subsequently, after investigations, Italy fined OpenAI €15 million in December 2024 for unlawful processing of user data and failure to comply with information obligations. The case presented shows that already in the absence of dedicated AI legislation, authorities are using the existing legal framework (GDPR) to penalise the unreasonable use of AI that infringes rights (in this case, the right to privacy and data protection). As a result, tech companies are forced to adopt proactive privacy by design measures in AI systems, integrating ethical and legal data considerations at the design stage.

The Digital Services Act (DSA) as Regulation (EU) 2022/2065 is called, applicable from February 2024, sets clear responsibilities for online platforms in managing illegal content and societal risks. Although the DSA is not AI-focused, it contains provisions concerning algorithmic automated recommendations and moderation systems. The DSA requires very large platforms (VLOPs, with more than 45 million users in the EU) to conduct annual assessments of the systemic risks of their services, including risks of dissemination of illegal content, negative impacts on fundamental rights, civic discourse, electoral processes or public health. They are risks often generated or amplified by the AI algorithms used by platforms (e.g. recommendation engines may favour misinformation or hate speech because they maximise engagement). The DSA requires platforms to take steps to mitigate identified risks and to submit to independent audits. Interestingly, the preamble of the DSA explicitly mentions the relevance of the UN Guiding Principles (UNGPs), and the obligations to assess risks and remediation measures are reminiscent of the due diligence process in the UNGPs[36]. Practically, the DSA transplants the concept of corporate responsibility for rights into a concrete digital context in that large technology companies must take steps to respect the rights of users and the public (such as freedom of expression, protection against discrimination, etc.) in the way their algorithms operate. We are therefore witnessing a paradigm shift from the past, when platforms

[35] Pollina, Elvira, and Armellini, Alvise, 'Italy Fines OpenAI over ChatGPT Privacy Rules Breach.' *Reuters*, 20 December 2024, Accessed May 2, 2025, https://www.reuters.com/technology/italy-fines-openai-15-million-euros-over-privacy-rules-breach-2024-12-20/.

[36] Ebert, Isabel. *Fostering Business Respect for Human Rights in AI Governance and Beyond: A Compass for Policymakers to Align Tech Regulation with the UNGPs*. Carr Center for Human Rights Policy, Harvard Kennedy School, Harvard University, 18 April 2024, Accessed May 2, 2025. https://www.hks.harvard.edu/sites/default/files/2024-04/24_Ebert_TechFellowPaper.pdf.

often hid behind the status of passive intermediaries. DSAs clarify that, given their systemic influence, they have active due diligence duties.

The Digital Markets Act (DMA), or Regulation (EU) 2022/1925, came into force in 2023 and aims to regulate fair and contestable digital markets by targeting gatekeepers (large companies that control key platforms, such as operating systems, app stores, major social networks and search engines). Although the DMA is competition-orientated and does not directly mention human rights, it contributes to holding tech giants accountable by prohibiting abusive practices and imposing transparency obligations. For example, gatekeepers are required to allow interoperability with third parties, to stop combining personal data from different services without consent (which is related to privacy protection), to make transparent algorithmic ranking policies in app stores or search engines, and to avoid self-favouring their own services. Indirectly, the DMA reinforces an environment in which corporate responsibility encompasses respect for principles of fairness and transparency in business practices, preventing excessive concentration of technological power that could lead to infringement of consumer rights or reduce pluralism (an essential element of a democratic society). Together with the DSA, the DMA reflects the EU's endeavour to establish a holistic digital governance framework, driven by the fact that tech companies are no longer only liable *post-factum* for concrete harms, but are subject to preventive oversight and standards of conduct aimed at protecting users, the market and fundamental rights.

From the regulations presented, it appears that the overall European regulatory regime is developing what we could call a digital corporate responsibility ecosystem. The GDPR protects data (the AI fuel) and that it is managed ethically and legally; the DSA governs how AI platforms influence discourse and information in society; the DMA maintains competition and freedom of choice in a digital economy dominated by large corporations; and the AI Act and the liability reforms discussed above directly address the development and use of artificial intelligence systems. Together, these instruments outline a system of obligations that, *de facto*, constitutes the elements of a new legal-ethical contract within which companies can innovate and thrive using AI, but, in return, must prevent abuses, respect rights, and be held accountable when things go wrong.

In practice, generative AI systems can be used in consumer markets both as stand-alone/autonomous products and embedded in complex products (products with digital elements). In use, these products can cause malfunctions leading to either personal injury, economic loss or data loss/damage or alteration. Therefore, the market launch of products with digital elements, including the presence of autonomous AI systems, should be accompanied by sufficient safeguards to minimise the risk of damage that these technologies may cause through their use.

In analysing this content, we start with the idea that liability rules have two functions in our society: on the one hand, they ensure that victims of third-party injuries receive compensation and, on the other hand, they provide economic incentives for the liable party to avoid causing harm. The rules on liability must always strike the right balance between the objective of protecting citizens and enabling businesses to innovate.

At this level the oft-heard question arises: who is liable for damages caused by AI systems? In order to avoid a ‘legislative vacuum[37] in terms of identifying who is liable, it is necessary to address the civil liability model for AI systems at the EU and even the international level, which is difficult to achieve uniformly.[38]

To the same extent, it raises questions as to how existing liability rules might apply to these new AI systems, so in a first approach, we might be tempted to opine that a complete overhaul of liability regimes is not necessary, as they are considered workable, but that the complexity opaqueness, the ability to be modified by updates, the capacity for autonomous learning and the potential autonomy of AI systems, as well as the large number of actors involved, constitute a significant challenge when analysing the effectiveness of existing EU and national liability regulatory instruments.[39]

Therefore, the need for the adoption of a harmonised framework stems from the fact that, *per a contrario*, in the absence of uniform rules at the EU level[40], for compensation for damage caused by defects in stand-alone or integrated product-integrated IA systems, suppliers, operators and users, on the one hand, and injured consumers, on the other hand, would be faced with 27 different liability regimes, leading to distinct levels of protection. The need for a coordinated reform at the EU level is also underpinned by the realisation that there are numerous obstacles stemming from the fact that those traders who wish to produce or operate AI-based products and services across borders are not aware or are insufficiently aware of national liability regimes for AI-related harm. Therefore, in a cross-border context, the present common liability framework will trigger the desired harmonisation and legal certainty while providing the necessary flexibility to allow Member States to integrate harmonised measures smoothly into their national liability regimes.

5. Relevant Case Law and Practical Problems in Holding Liable

As many of the regulations mentioned are very recent or even not yet fully in force (e.g. The AI Act will effectively apply from 2026, as will the new Product Directive), specific case law on AI and corporate liability is only just beginning to take shape. However, there are already a few landmarks and cases that foreshadow how courts and authorities will interpret the new legal-ethical framework. A first set of precedents comes from the application of existing regulations to situations where AI

[37] Nevejans, Nathalie, Treatise on law and ethics for civil robotics/*Traité de droit et d’éthique de la robotique civile*, LEH, 2017, p. 553 et seq.

[38] Novelli, Claudio, Casolari, Federico, Hacker, Philipp, Spedicato, Giorgio and Floridi, Luciano, "Generative AI in E U Law: Liability, Privacy, Intellectual Property, and Cybersecurity." *Computer Law & Security Review* 55 (November 2024): 106,066, Accessed May 5.2025. https://doi.org/10.1016/j.clsr.2024.106066.

[39] See in this regard van der Merwe, Matthew, Ketan Ramakrishnan, and Markus Anderljung. "Tort Law and Frontier AI Governance." *Lawfare*, May 24, 2024. Accessed June 6, 2025. https://www.lawfaremedia.org/article/tort-law-and-frontier-ai-governance.

[40] For the specificities of the European Union as a new legal typology, see Laura-Cristiana Spătaru-Negură, *European Union Law – a new legal typology/Dreptul Uniunii Europene – o nouă tipologie juridică, Hamangiu Publishing House*, 2016, Bucharest.

has been involved. The OpenAI/ChatGPT vs. Garante (Italy) case mentioned above is relevant in that the data protection authority acted promptly against a service based on generative AI, ruling that users' rights (such as information and consent to data processing) also prevail in the context of new technologies. The Garante decision, confirmed by the imposition of the fine, sends a clear message to the industry: launching an innovative AI model does not relieve a company from its traditional legal responsibilities towards users[41]. As a result, authorities in other EU countries (France and Spain) have opened investigations into facial recognition or AI employee monitoring technologies, indicating that data protection and labour law principles fully apply in the AI era.

5.1. Responsibility for Online Content

Previous DSA case law has paved the way for increased accountability of platforms, albeit indirectly. Cases such as Delfi AS v. Estonia (ECtEDO, 2015)[42] where a news platform was held liable for offensive comments posted anonymously by users, or Glawischnig-Piesczek v. Facebook (CJEU, 2019),[43] which allowed platforms to be ordered to remove globally defamatory content similar to that already declared illegal, show a trend away from the old model of near-total immunity of intermediaries. The two judgements, while not directly concerning AI, are relevant because many platforms use AI to moderate content. Implicitly, if platforms are held liable for illegal content, they will have to solve the problem that their algorithmic tools effectively detect and remove that content. The DSA comes precisely to codify these proactive obligations, confirming the jurisprudential direction.

5.2. Liability for Products with IA Components

A possible precursor is the case law on semi-autonomous vehicles. As an example, accidents involving (AI-based) autopilot systems have resulted in legal actions against car manufacturers. In the absence of the new Directive 2024/2853, such cases are dealt with legally, either contractually or by classical tort law, but courts have started to take note of the difficulties of establishing fault in the software context. It is anticipated that once the new Directive is implemented, litigation of this type will shape due diligence standards for manufacturers of autonomous vehicles, robots, smart medical devices, etc., and companies will need to demonstrate that they have complied with state-of-the-art science and cybersecurity requirements to avoid liability.

Another important issue is access to justice and proof in AI cases. In the past,

[41] Pollina, Elvira, and Alvise Armellini. 'Italy Fines OpenAI over ChatGPT Privacy Rules Breach.' *Reuters*, 20 December 2024. Accessed May 2, 2025. https://www.reuters.com/technology/italy-fines-openai-15-million-euros-over-privacy-rules-breach-2024-12-20/.

[42] *Delfi AS v. Estonia*, no. 64,569/09 European Court of Human Rights (Grand Chamber), 16 June 2015. Accessed May 7, 2025. https://hudoc.echr.coe.int/fre?i=001-155105.

[43] *Eva Glawischnig – Piesczek v. Facebook Ireland Limited*, C-18/18, Court of Justice of the European Union, 3 October 2019. Accessed May 7, 2025. https://curia.europa.eu/jcms/jcms/p1_2434826/en/.

companies could invoke the trade secrecy of algorithms to block investigations or technical expertise. Now, with the new rules (AI Act, AI Directive) allowing court orders for disclosure, case law on the balance between algorithmic transparency and intellectual property protection is emerging. Courts will have to establish protocols whereby independent experts can audition disputed source code or AI models without jeopardising companies' proprietary rights, while respecting victims' due process rights. Basically, this is an area with few concrete precedents, but the critic is determining how, practically speaking, the victim will be able to prove fault in the loop, i.e. that a particular design or lack of diligence by the company in developing the AI caused the harm.

Not all countries are moving at the same pace as the EU, so forum shopping (choice of jurisdiction) could become a phenomenon where victims of AI injuries will prefer to sue companies in countries with more favourable legal regimes (such as the EU). As a result, global companies will be forced to meet the highest standards to avoid exposure. Already, large tech firms have begun to align their internal policies with UNGPs and EU regulations, recognising that the regulatory tide is going global. As Isabel Ebert observes, the fact that industry leaders are voluntarily adopting a human rights-based approach to risk management indicates that regulations anchored in the UNGPs can be implemented in practice and create the foundation for rights-respecting AI practices[44]. In other words, ethical norms become de facto norms, either through internalisation by companies under pressure of societal expectations or through legal transposition.

5.3. About Significant Technological Issues

The concept of a pacing problem (the speed gap between technology and law) suggests that new AI applications will soon emerge for which current regulations do not provide clear solutions. One such example is the rise of generative AI (such as large language models that can produce text, images and code). Obviously, these raise issues of intellectual property (plagiarisation of training data), automated defamation, and deepfakes that can damage democratic processes or reputations. To what extent do companies that provide such models for user-generated content respond? Recently, lawsuits have been filed in the US against OpenAI and Meta for defamatory outputs or for using copyrighted data in training, issues on the regulatory borderline. Europe, through the AI Act, partially addresses the phenomenon (transparency and copyright requirements on general generation models)[45], but how courts will construct legal liability (is the model a mere neutral tool or does the company have a post-release duty of control over how it is used?) will require legal innovation.

[44] Ebert, Isabel, *Fostering Business Respect for Human Rights in AI Governance and Beyond: A Compass for Policymakers to Align Tech Regulation with the UNGPs* (Carr Center for Human Rights Policy, Harvard Kennedy School, Harvard University, 18 April 2024), Accessed May 7, 2025, https://www.hks.harvard.edu/sites/default/files/2024-04/24_Ebert_TechFellowPaper.pdf.

[45] European Commission. 'Regulatory Framework for Artificial Intelligence.' *Shaping Europe's Digital Future*. Accessed May 7, 2025. https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai.

5.3.1. The Criminal Dimension of Liability

If an AI system causes death or injury due to developer negligence, can criminal charges be brought? The concept of crimes of omission (e.g. deliberate failure to deploy safety guards) could evolve to cover AI cases. Already, in the context of autonomous vehicles, the criminal liability of manufacturers or operators in case of fatal accidents is being discussed, especially if ignorance of technical warnings is proven. Presumably, with the eventual UN Treaty providing for the extension of liability to legal entities[46] and criminally, we could see companies criminally charged for serious AI-related incidents (similar to how companies can be criminally charged for environmental disasters or industrial accidents). Or it is precisely the emerging case law that confirms the general direction towards a destination where companies are expected (and increasingly obliged) to anticipate and prevent the negative effects of AI technologies and to take responsibility when such effects nevertheless occur. Access to remedies for victims is becoming a central principle, either through modernised civil liability regimes or quasi-judicial mechanisms (OECD contact points, regulators). Courts are beginning to require from companies a level of due diligence comparable to that of a prudent professional (updated 21st-century family father diligence) in the design and implementation of AI.

6. Conclusions

The transformations analysed indicate that we are in the process of establishing a new legal-ethical contract between corporations and society regarding artificial intelligence. 'The "contract", although used metaphorically for the time being, is far from being purely formal, but is in the process of becoming, resulting from the convergence of legal norms, ethical standards and public expectations that shape the acceptable limits of corporate action when AI is involved, with a potential impact on human rights.

Artificial intelligence has acted as a trigger for rethinking corporate responsibility. While in the past companies could argue that they had no role in guaranteeing human rights (that is the remit of states) and that they were only accountable to shareholders, today this argument is no longer tenable. The proliferation of AI in all sectors, from health to justice, from social networks to finance, has demonstrated that algorithmic decisions and actions can profoundly affect the dignity, privacy, equal opportunities, security and other rights of individuals. Therefore, companies that develop or use AI are subject, explicitly or implicitly, to the obligation to prevent abuses and to respect the ethical-legal parameters set by society. The new contract manifests itself on several concrete levels, highlighted throughout the paper, the first of which is the normative level, moving from voluntary recommendations to legal obligations. The UN guiding principles and OECD standards, while remaining

[46] See Muñoz Quick, Paloma. 'Levelling the Global Playing Field: A Binding Treaty on Business and Human Rights.' *BSR*, 25 January 2024. Accessed May 9, 2025. https://www.bsr.org/en/blog/leveling-the-global-playing-field-a-binding-treaty-on-business-and-human-rights.

basic references, are now doubled by laws and possible treaties that *force* compliance. The room for manoeuvre for companies willing to ignore human rights is narrowing considerably. The EU, with its advanced legislation (AI Act, DSA, etc.), has created a *de facto* mandatory due diligence regime for digital rights. At the global level, if adopted, the UN treaty will generalise this approach, possibly instituting cross-border sanctions for companies that fail to meet their responsibilities.

The second level is procedural, by rebalancing victims' chances of obtaining remedies, as the new contract no longer admits grey areas of technological impunity. The presumptions of causation in favour of victims, the transparency imposed on algorithms and the extension of the concept of defect to cybersecurity all show a clear intention to dismantle the barriers that, until now, protected AI developers from liability. It is thus recognised that innovation cannot be an excuse for neglecting the principle of reparation for harm suffered by individuals. In contractual terms, if society accepts the introduction of AI into its everyday life, companies promise (through laws and codes of ethics) that they will not leave individuals stranded in the face of the adverse consequences of AI.

The institutional level is the third and manifests itself in the creation of new oversight mechanisms and authorities where the legal-ethical contract takes the form of a governance regime in which both public institutions (AI oversight agencies, data protection authorities, independent audit bodies under the DSA) and multi-stakeholder mechanisms (such as OECD National Contact Points, or future AI centres of expertise) interact to monitor and guide companies' behaviour. Basically, a collective but distributed responsibility is being structured whereby companies have the primary duty of compliance and self-reporting, and the institutions monitor and intervene correctively. The new responsibility reflects a maturing of the market as tech companies become as regulated on *compliance* considerations as the financial or pharmaceutical industries.

The last level is the cultural one, materialised in the change of discourse within companies and the business environment, where notions such as 'AI ethics', 'corporate digital responsibility' and 'human rights by design' are gaining ground. Large corporations are hiring AI ethics officers, forming advisory boards of human rights experts and issuing digital sustainability reports. These are all signs that social norms align with the new legal norms and companies are expected to not only comply with the letter of the law, but also the spirit of the law, integrating respect for human dignity into their business model. In a way, the pressure is also coming from the bottom up, as users, consumers and employees are demanding that technology is used responsibly. The ethical contract implies, along with minimum legal obligations, the legitimate expectation that firms will do the right thing, even beyond what is strictly required.

Of course, this new contract is in its infancy and will require continuous fine-tuning. Technological innovation will constantly test the boundaries of regulation, so from general AI to AI-augmented biotechnology, new areas will raise questions that today we do not have answers to. Additional international instruments may be needed, such as a global Treaty on Artificial Intelligence (already the Council of Europe has agreed in 2024 on a Framework Convention on AI and Human Rights, the first treaty dedicated to AI at the international level)[47], which would complete the current patchwork of regulations and set a common standard for states and companies, preventing fragmentation of rules.

Another aspect to watch remains how concrete cases laws in different jurisdictions will interpret the new obligations. International harmonisation will not be immediate because of differences such as the American approach based on self-regulation and *post-facto* remedies, which differ from the European preventive approach. But in the long term, it is expected that the principles of due diligence, transparency and remediation will become universal. The ethical-legal contract will develop practices and precedents that will push companies towards a proactive compliance model. In conclusion, the slogan 'corporate liability in the AI era' is no longer just a matter of legal reaction after harm has occurred, but is becoming an adapted regime of anticipatory governance. Companies that adopt AI are copartners, alongside states and civil society, in a digital social contract where innovation and the harnessing of algorithmic power come hand in hand with the commensurate assumption of ethical and legal responsibilities. It is only through this balance that a genuine ethical-legal contract produces its legal effect for technological progress realised in the service of human beings, and not to their detriment.

Bibliography

1. Almada, Marco, and Nicolas Petit. 'The EU AI Act: Between the Rock of Product Safety and the Hard Place of Fundamental Rights.' *Common Market Law Review,* 62, no. 1 (2025): 85–120, Accessed May 8, 2025, https://kluwerlawonline.com/journal article/Common+Market+Law+Review/62.1/COLA2025004.
2. Bacciarelli Anna and Aufiero, Paul, 'Pandora's Box: Generative AI Companies, ChatGPT, and Human Rights,' *Human Rights Watch*, 3 May 2023, Accessed May 9, 2025, https://www.hrw.org/news/2023/05/03/pandoras-box-generative-ai-companies-chatgpt-and-human-rights.
3. Cooley L. L P. 'OECD Guidelines on Responsible Business Conduct: Key Considerations for Multinational Enterprises.' *Cooley*, May 31, 2024, Accessed May 9, https://www.cooley.com/news/insight/2024/2024-05-31-oecd-guidelines-on-responsible-business-conduct-key-considerations-for-multinational-enterprises
4. *Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*. Council of Europe Treaty Series – No. 225. Strasbourg: Council of Europe, 2024. Accessed May 2, 2025. https://rm.coe.int/1680afae3c.

[47] Council of Europe *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*. Council of Europe Treaty Series – No. 225. Strasbourg: Council of Europe, 2024. Accessed May 2, 2025. https://rm.coe.int/1680afae3c. Also see Presno Linera, Miguel Ángel, and Anne Meuwese. 2025. "Regulating AI from Europe: A Joint Analysis of the AI Act and the Framework Convention on AI." *The Theory and Practice of Legislation*, April 1–20. doi:10.1080/20508840.2025.2492524 and Marcu, Bianca-Ioana. "The World's First Binding Treaty on Artificial Intelligence, Human Rights, Democracy, and the Rule of Law: Regulation of AI in Broad Strokes." *Future of Privacy Forum*, June 20, 2024. Accessed May 5, 2025. https://fpf.org/blog/the-worlds-first-binding-treaty-on-artificial-intelligence-human-rights-democracy-and-the-rule-of-law-regulation-of-ai-in-broad-strokes/.

5. *Delfi AS v. Estonia*, no. 64,569/09 European Court of Human Rights (Grand Chamber), 16 June 2015. Accessed 7 May 2025. https://hudoc.echr.coe.int/fre?i=001-155105.
6. European Union. *Directive (EU) 2024/2853 of 23 October 2024 on Liability for Defective Products and Repealing Council Directive 85/374/EEC*. *Official Journal of the European Union*, L 2853, November 18, 2024. Accessed June 6, 2025. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024L2853.
7. Duffourc, Marie-Naëlle, and Gerke, Sara, '*The Proposed EU Directives for AI Liability Leave Worrying Gaps Likely to Impact Medical AI.' NPJ Digital Medicine* 6 (2023): 77, Accessed May 9, 2025, https://doi.org/10.1038/s41746-023-00823-w.
8. Duffourc, Mindy Nunez Nunez and Gerke, Sara, The Proposed EU Directives for AI Liability Leave Worrying Gaps Likely to Impact Medical AI' *npj Digital Medicine* 6, (2023): 77, Accessed May 9, 2025, https://www.nature.com/articles/s41746-023-00823-w.
9. Ebert, Isabel. 'Fostering Business Respect for Human Rights in AI Governance and Beyond: A Compass for Policymakers to Align Tech Regulation with the UNGPs.' Carr Center Discussion Paper, Issue 2024-05. Harvard Kennedy School, Harvard University, April 18, 2024, Accessed May 9, 2025, https://www.hks.harvard.edu/sites/default/files/2024-04/24_Ebert_TechFellowPaper.pdf.
10. *Eva Glawischnig – Piesczek v. Facebook Ireland Limited*, C-18/18, Court of Justice of the European Union, 3 October 2019. Accessed May 7, 2025. https://curia.europa.eu/jcms/jcms/p1_2434826/en/.
11. Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework, UN Doc. A/HRC/17/31 (2011). https://www.ohchr.org/sites/default/files/Documents/Issues/Business/A-HRC-17-31_AEV.pdf
12. Guidelines for Multinational Enterprises, 2011 Edition (Paris: OECD Publishing, 2011), https://www.oecd.org/en/publications/oecd-guidelines-for-multinational-enterprises-on-responsible-business-conduct_81f92357-en.html.
13. Yazici, Tuana, 'Toward a Global Standard for Ethical AI Regulation: Addressing Gaps in AI-Driven Biometric and High-Resolution Satellite Imaging in the EU AI Act.' *Law, Innovation and Technology* 17 (1) (2025): 366–394. Accessed May 5, 2025, https://www.tandf online.com/doi/full/10.1080/17579961.2025.2470589
14. ISACA, *Understanding the EU AI Act: Requirements and Next Steps* (Schaumburg, IL: ISACA, 18 October 2024), https://www.isaca.org/resources/white-papers/2024/understanding-the-eu-ai-act.
15. Latham & Watkins L. L P. *New EU Product Liability Directive Comes Into Force*. Client Alert No. 3319. December 23, 2024, Accessed May 5, 2025, https://www.lw.com/en/offices/admin/upload/SiteAttachments/New-EU-Product-Liability-Directive-Comes-Into-Force.pdf.
16. 'Liability Rules for Artificial Intelligence.' *European Commission*, Accessed May 10, 2025. https://commission.europa.eu/business-economy-euro/doing-business-eu/contract-rules/digital-contracts/liability-rules-artificial-intelligence_en.
17. Liebholz, Alina, 'Commentary: Who is Liable if AI Violates Your Human Rights?,' *Impakter*, reprinted from *Business & Human Rights Resource Centre*, 28 May 2023, Accessed May 5, 2025, https://www.business-humanrights.org/en/latest-news/company-liability-for-human-rights-violations-caused-by-ai/.
18. Markoff, Tyler. 'The First of Its Kind: The EU AI Act and What It Means for the Future of AI.' *Fordham Journal of Corporate & Financial Law*, April 23, 2024. https://news.law.fordham.edu/jcfl/2024/04/23/the-first-of-its-kind-the-eu-ai-act-and-what-it-means

-for-the-future-of-ai/

19. Marcu, Bianca-Ioana. "The World's First Binding Treaty on Artificial Intelligence, Human Rights, Democracy, and the Rule of Law: Regulation of AI in Broad Strokes." *Future of Privacy Forum*, June 20, 2024. Accessed May 5, 2025. https://fpf.org/blog/the-worlds-first-binding-treaty-on-artificial-intelligence-human-rights-democracy-and-the-rule-of-law-regulation-of-ai-in-broad-strokes/.
20. Martin, Baily. "Privacy in a Programmed Platform: How the General Data Protection Regulation Applies to the Metaverse." *Harvard Journal of Law & Technology* 36, no. 1 (Fall 2022): 235–261. Accessed June 6, 2025. https://jolt.law.harvard.edu/assets/articlePDFs/v36/Martin-Privacy-in-a-Programmed-Platform.pdf.
21. Van der Merwe, Matthew, Ketan Ramakrishnan, and Markus Anderljung. "Tort Law and Frontier AI Governance." *Lawfare*, May 24, 2024. Accessed June 6, 2025. https://www.lawfaremedia.org/article/tort-law-and-frontier-ai-governance.
22. Mingrone, Francesca, and Suárez-Franco, Ana María, 'Grounding the new legally binding instrument on transnational corporations on the right to a healthy environment', *Third World Resurgence*, no. 362 (March 2025), Accessed May 5, 2025, https://twn.my/title2/resurgence/2025/362/cover03.htm.
23. Muñoz Quick, Paloma, 'Leveling the Global Playing Field: A Binding Treaty on Business and Human Rights,' *BSR – Business for Social Responsibility*, 25 January 2024, Accessed May 9, 2025, https://www.bsr.org/en/blog/leveling-the-global-playing-field-a-binding-treaty-on-business-and-human-rights.
24. Ness, James., 'EU's AI Act Fails to Set Gold Standard for Human Rights.' *European Disability Forum*, April 3, 2024, Accessed May 9, 2025, https://www.edf-feph.org/publications/eus-ai-act-fails-to-set-gold-standard-for-human-rights/.
25. Nevejans, Nathalie, Traité *de droit et d'*éthique *de la* robotique civile/*Traité de droit et d'éthique de la robotique civile* (LEH, 2017) : 553 et seq.
26. Nina M Hart, Christopher A Casey, Transatlantic leadership in an era of human rights-based export controls, *Journal of International Economic Law*, Volume 27, Issue 1, March 2024, pp. 130–146, https://doi.org/10.1093/jiel/jgae005
27. Novelli, Claudio, Casolari, Federico, Hacker, Philipp, Spedicato, Giorgio and Floridi, Luciano, "Generative AI in E U Law: Liability, Privacy, Intellectual Property, and Cybersecurity." *Computer Law & Security Review* 55 (November 2024): 106066. Accessed May 5, 2025. https://doi.org/10.1016/j.clsr.2024.106066.
28. Piasecki, Stanislaw, and Helberger, Natali, 'A Nightmare to Control: Legal and Organisational Challenges around the Procurement of Journalistic AI from External Technology Providers.' *The Information Society* 41 (3) (2025): 173–194. Accessed May 2, 2025, https://www.tandfon line.com/doi/full/10.1080/01972243.2025.2473398.
29. Presno Linera, Miguel Ángel, and Anne Meuwese. 2025. "Regulating AI from Europe: A Joint Analysis of the AI Act and the Framework Convention on AI." *The Theory and Practice of Legislation*, April, 1–20. doi:10.1080/20508840.2025.2492524.
30. Pollina, Elvira, and Armellini, Alvise, 'Italy Fines OpenAI over ChatGPT Privacy Rules Breach.' *Reuters*, 20 December 2024. Accessed May 2, 2025. https://www.reuters.com/technology/italy-fines-openai-15-million-euros-over-privacy-rules-breach-2024-12-20/.
31. *Proposal for a Directive of the European Parliament and of the Council on Adapting Non-Contractual Civil Liability Rules to Artificial Intelligence (AI Liability Directive).* COM (2022) 496 final, September 28, 2022. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0496.
32. Regulation (EU) 2024/1689 of 13 June 2024, Laying Down Harmonised Rules on

Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). Official Journal of the European Union L 2024/1689, 12 July 2024, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689.

33. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act), Official Journal of the European Union, L 277/1, 27 October 2022, https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng.
34. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on Contestable and Fair Markets in the Digital Sector (Digital Markets Act), Official Journal of the European Union, L 265/1, 12 October 2022, https://eur-lex.europa.eu/eli/reg/2022/1925/oj/eng.
35. European Union. *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 – GDPR)*. *Official Journal of the European Union*, L 119/1, May 4, 2016. Accessed June 6, 2025. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.
36. 'Regulatory Framework for Artificial Intelligence.' *Shaping Europe's Digital Future*. Accessed May 7, 2025. https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai.
37. Schuett, Jonas. "Risk Management in the Artificial Intelligence Act." *European Journal of Risk Regulation* 15, no. 2 (2024): 367–85. https://doi.org/10.1017/err.2023.1.
38. Spătaru-Negură, Laura-Cristiana. *European Union Law – a new legal typology// Dreptul Uniunii Europene – o nouă tipologie juridică*, Hamangiu Publishing House, 2016, Bucharest.
39. Tyler, Markoff "The First of Its Kind: The EU AI Act and What It Means for the Future of AI." *Fordham Journal of Corporate & Financial Law*, April 23, 2024, Accessed May 9, 2025, https://news.law.fordham.edu/jcfl/2024/04/23/the-first-of-its-kind-the-eu-ai-act-and-what-it-means-for-the-future-of-ai/.
40. United Nations Binding Treaty on Business and Human Rights: FIDH's Position Ahead of the 10th Negotiation Session, *FIDH*, July 2023, Accessed May 2, 2025, https://www.fidh.org/en/issues/business-human-rights-environment/business-and-human-rights/un-binding-treaty-position-2023.
41. Updated February 2025 Roadmap and Methodology for the Implementation of HRC Decision 56/116. February 2025, Accessed May 2, 2025, https://media.business-humanrights.org/media/documents/Updated_Feb_2025-Roadmap_and_Methodology_IGWG_treaty.pdf.