NORDIC JOURNAL OF EUROPEAN LAW

Volume 8
Issue 3· 2025

LUND UNIVERSITY
HELSINGIN YLIOPISTO
UNIVERSITY OF BERGEN
SDU
UPPSALA UNIVERSITET
ISSN 2003-1785

NORDIC JOURNAL OF EUROPEAN LAW
ISSUE N 3 OF 2025

http://journals.lub.lu.se/njel

University of Bergen, University of Copenhagen, University of Helsinki, Lund University, Reykjavik University, University of Southern Denmark, Uppsala University

TABLE OF CONTENTS

ARTICLES

REVIEWS AND INTERVIEWS

THE EU's MUTUAL DEFENCE CLAUSE: LEGAL AND STRATEGIC CONSIDERATIONS ON ARTICLE 42(7) TEU IN AN AGE OF RENEWED MILITARY THREATS

FEDERICA FAZIO*

EU institutions have expanded their involvement in defence since 2016, prompted by Brexit and Donald Trump's first presidential victory. This trend has become even more pronounced since the 2022 Russian invasion of Ukraine. NATO remains central to Europe's territorial defence, as evidenced by Finland and Sweden's accession, yet there also exists legal basis for the EU to play a role. Article 42(7) of the Treaty on European Union (TEU) obliges Member States to assist each other in the event of armed aggression, echoing Article 5 of the North Atlantic Treaty (NAT). This provision has received limited attention from legal scholars. With the war in Ukraine intensifying, concerns over Trump undermining Article 5 NAT and rising risks of military and hybrid attacks on Europe, it is crucial to understand how the EU's mutual defence clause would be implemented. This includes its interplay with the EU's solidarity clause in Article 222 of the Treaty on the Functioning of the EU (TFEU) and NATO's own mutual defence clause. To this end, this article undertakes a legal and strategic analysis of Article 42(7) TEU. Following an introduction that outlines the topic and methodology, Section 1 offers a legal perspective, while Section 2 a strategic perspective. Section 3 concludes that, while significant progress has been made, the EU is not yet in a position to credibly threaten the use of force in the exercise of collective defence.

INTRODUCTION

In 1991, then-Belgian Minister of Foreign Affairs, Mark Eyskens, described the EU as 'an economic giant, a political dwarf and a military worm'.[1] Today, the EU is no longer a political dwarf or a military worm, though military capability shortfalls remain.

---

* PhD Candidate in the School of Law and Government at Dublin City University (DCU) and Academic Assistant in the European Legal Studies Department at the College of Europe in Bruges.
The author is deeply grateful to Prof Federico Fabbrini and Dr Kenneth McDonagh at DCU, for their invaluable insights and guidance in the development of this article, as well as to Prof Ben Tonra at University College Dublin for his insightful comments and continued support. The author would also like to thank Prof Michal Onderco and Drs Daniel Fiott, Joris Larik, Eva Kassoti, Narin Idriz and Niels Kirst for their helpful comments, and the Editor-in-Chief, Dr Alezini Loxa, for her interest in this article and kind assistance throughout the review process. Part of this paper was presented at the PhD workshop "The legal implications of the EU's geopolitical awakening"', jointly organised by the Asser Institute's Centre for the Law of EU External Relations (CLEER) and Leiden University College The Hague on 14-15 November 2024. It was subsequently published as a Working Paper in an edited volume of the same name in the CLEER paper series in March 2025.
This research was supported by a Marie Curie Staff Exchange within the Horizon Europe Programme (grant acronym: ORCA, no: 101182752).
[1] As quoted by Craig R Whitney, 'War in the Gulf: Europe; Gulf Fighting Shatters Europeans' Fragile Unity', (The New York Times, 25 January 1991) <https://www.nytimes.com/1991/01/25/world/war-in-the-gulf-europe-gulf-fighting-shatters-europeans-fragile-unity.html> accessed 20 September 2024.

In 2007, the Lisbon Treaty modified the 1992 Maastricht Treaty (or TEU) – as well as the other founding treaty, the Treaty Establishing the European Community (TEC), which it renamed as TFEU – and transformed the European Security and Defence Policy (ESDP), establishing the Common Security and Defence Policy (CSDP). Outlined in Articles 42-46 of Title V, Section 2, the CSDP has made security and defence an integral part of the Common Foreign and Security Policy (CFSP) intergovernmental framework and allows EU Member States to make security and defence policy decisions on the basis of unanimity.[2]

While reaffirming the Maastricht Treaty's principle that a common defence policy would develop progressively, with a common defence requiring unanimous agreement by the European Council,[3] the Lisbon Treaty introduced a mutual assistance obligation for EU Member States in Article 42(7) TEU. This obligation requires Member States to assist one another in the event of an armed aggression. Consequently, although the failure of the 1952 European Defence Community project means that the EU lacks a common defence – such as NATO's integrated military command structure, shared nuclear doctrine, and other traditional defensive alliance characteristics – the EU Treaty now includes a qualified mutual defence clause.

Despite acknowledging that NATO remains the cornerstone of territorial defence for those countries who are members of both organisations, the 2016 EU Global Strategy and, more recently, the 2022 Strategic Compass, have stressed the need for EU Member States to be prepared to translate mutual assistance commitments into action.[4] The strategic autonomy envisaged in 2016 remains largely a work in progress, as highlighted by the continued need to negotiate and align with the US, exemplified by the EU-US Framework on Reciprocal, Fair, and Balanced Trade announced in August.[5] Yet, the EU has clearly made considerable steps forward, particularly since Russia launched an all-out war against Ukraine on 24 February 2022.[6]

The Union has supplied Ukraine with €11.1 billion in military aid through the European Peace Facility (EPF), an off-budget fund which enabled it to provide lethal weapons for the first time,[7] and launched a training mission for Ukrainian forces on its soil,

---

[2] Consolidated version of the Treaty on European Union [2016] OJ C 202/38 (TEU) Article 42(4).
[3] Ibid Article 42(2); Treaty on European Union [1992] OJ C191/59 Article J.4(1).
[4] European External Action Service, 'Shared Vision, Common Action: A Stronger Europe: A Global Strategy for the European Union's Foreign and Security Policy' (June 2016) (EUGS) 9, 14, 19 and 20 <https://www.eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf> accessed 20 September 2024; European External Action Service, 'A Strategic Compass for Security and Defence. For a European Union that protects its citizens, values and interests and contributes to international peace and security' (March 2022) 10, 14, 23, 28, 30, 31, 34, 35, 36, 39, 40, 53 and 54, <https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf> accessed 20 September 2024.
[5] Europea Commission, 'Joint Statement on a United States-European Union framework on an agreement on reciprocal, fair and balanced trade', Statement, (21 August 2025), available <https://policy.trade.ec.europa.eu/news/joint-statement-united-states-european-union-framework-agreement-reciprocal-fair-and-balanced-trade-2025-08-21_en> accessed 23 September 2025.
[6] See, e.g., Federico Fabbrini, 'To "Provide for the Common Defence": Developments in Foreign Affairs and Defence' in Federico Fabbrini (ed), The EU Constitution in Time of War (Oxford University Press, 2025) 21–47; Daniel Fiott, 'In every crisis an opportunity? European Union integration in defence and the War on Ukraine' (2023) 45(3) Journal of European Integration 447.
[7] Council of the EU, 'European Peace Facility: Timeline – European Peace Facility' (Last review: 4 December 2024) <https://www.consilium.europa.eu/en/policies/european-peace-facility/> accessed 7 January 2025; see also Federico Fabbrini, 'Funding the War in Ukraine, the European Peace Facility, the Macro-Financial Assistance Instrument, and the Slow Rise of and EU Fiscal Capacity' (2023) 11(4) Politics & Governance 52.

another first.[8] The EU has also introduced initiatives like the European Defence Industry Reinforcement through common Procurement Act (EDIRPA)[9] to address capability gaps, the Act in Support of Ammunition Production (ASAP)[10] to boost artillery shell production, the European Defence Industry Strategy (EDIS),[11] its first defence industrial strategy, supported by the European Defence Industry Programme (EDIP)[12] for long-term readiness, and, more recently, the ReArm Europe Plan/Readiness 2030[13] to facilitate national defence budget increases. Additionally, the Strategic Compass envisions the creation of a Rapid Deployment Capacity (RDC) of 5,000 troops by 2025.[14]

Therefore, the EU has adopted important defence initiatives and, by endangering the credibility of NATO's Article 5 security guarantee, the second Trump administration is likely to accelerate this trend further.

In light of these developments, this article aims to review the EU's mutual assistance clause, enshrined in Article 42(7) TEU, using a law-in-context approach.[15] The article is

---

[8] Council of the EU, 'Ukraine: EU launches Military Assistance Mission' (Press Release, 15 November 2022) <https://www.consilium.europa.eu/en/press/press-releases/2022/11/15/ukraine-eu-launches-military-assistance-mission/> accessed 20 September 2024.

[9] European Commission, 'Commission Implementing Decision of 15.3.2024 on the Financing of the Instrument for the Reinforcement of the European Defence Industry through Common Procurement (EDIRPA) Established by Regulation (EU) 2023/2418 of the European Parliament and of the Council and the Adoption of the Work Programme for 2024-2025' C(2024) 1700 final <https://defence-industry-space.ec.europa.eu/document/download/8b38112b-a9e2-499e-bb1e-b8dbfc6dfb27_en?filename=EDIRPA%20Implementing%20Decision%20EN.pdf> accessed 20 September 2024.

[10] European Commission, 'Commission Implementing Decision of 18.10.2023 on the Financing of the Instrument on Supporting Ammunition Production (ASAP) Established by Regulation (EU) 2023/1525 of the European Parliament and of the Council and the Adoption of the Work Programme for 2023-2025' C(2023) 7320 final <https://defence-industry-space.ec.europa.eu/document/download/5845b34d-bb2f-4381-aca3-ec9ff965f687_en?filename=C_2023_7320_1_EN_ACT_and_annex.pdf> accessed 20 September 2024.

[11] European Commission, 'Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A New European Defence Industrial Strategy: Achieving EU Readiness Through a Responsive and Resilient European Defence Industry' JOIN(2024) 10 final (5 March 2024) <https://defence-industry-space.ec.europa.eu/document/download/643c4a00-0da9-4768-83cd-a5628f5c3063_en?filename=EDIS%20Joint%20Communication.pdf> accessed 20 September 2024.

[12] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council establishing the European Defence Industry Programme and a framework of measures to ensure the timely availability and supply of defence products ('EDIP')' COM(2024) 150 final (5 March 2024)<https://defence-industry-space.ec.europa.eu/document/download/6cd3b158-d11a-4ac4-8298-91491e5fa424_en?filename=EDIP%20Proposal%20for%20a%20Regulation.pdf> accessed 20 September 2024.

[13] European Commission, 'Letter by President von der Leyen on defence' (4 March 2025) <https://ec.europa.eu/commission/presscorner/api/files/attachment/880628/Letter%20by%20President%20von%20der%20Leyen%20on%20defence.pdf> accessed 20 September 2024; see also European Commission, 'Communication from the Commission Accommodating increased defence expenditure within the Stability and Growth Pact' C(2025) 2000 final (19 March 2025) <https://defence-industry-space.ec.europa.eu/document/download/a57304ce-1a98-4a2c-aed5-36485884f1a0_en?filename=Communication-on-the-national-escape-clause.pdf> accessed 7 April 2025; European Commission, 'Proposal for a Council Regulation establishing the Security Action for Europe (SAFE) through the reinforcement of European defence industry Instrument' COM(2025) 122 final (19 March 2025) <https://defence-industry-space.ec.europa.eu/document/download/6d6f889c-e58d-4caa-8f3b-8b93154fe206_en?filename=SAFE%20Regulation.pdf> accessed 7 April 2025.

[14] EEAS, 'A Strategic Compass for Security and Defence' (n 4) 6, 11, 25, and 31.

[15] Megan Donaldson, 'Peace, war, law: teaching international law in contexts' (2022) 18(4) International Journal of Law in Context 393; Peter Cane, 'Context, context everywhere' (2020) 16(4) International Journal

structured as follows. The next Section provides a legal analysis of Article 42(7) TEU and the collective defence responsibilities it entails for EU members, including differences and overlaps with similar obligations under Article 222 TFEU and Article 5 NAT. The legal analysis shows that, similarly to Article 5 NAT, Article 42(7) TEU envisages an *obligation of result, not of means* but no disciplinary measures are contemplated in the event of inaction or inadequate action by one or more Member States. Furthermore, Article 42(7) TEU, like Article 5 NAT, covers both conventional and unconventional attacks – including cyber, hybrid, and space attacks, as well as state-sponsored and non-state sponsored terrorist attacks. This article, however, argues that the defence obligations triggered by the invocation of Article 42(7) TEU are *automatic*, unlike those under Article 5 NAT, *but not*, as some authors have suggested,[16] *unconditional*, due to the presence of both the Irish and NATO clauses.

The article concludes with a strategic analysis supporting a broad interpretation of Article 42(7) TEU, under whose scope both conventional and unconventional forms of aggression fall. To support this view, the article examines the EU's latest security strategies – the 2016 EU Global Strategy (EUGS) and the 2022 Strategic Compass – along with their associated implementation strategies and progress reports. These documents reveal, however, that the EU has consistently prioritised asymmetric threats such as terrorism, cyberattacks, hybrid warfare and space-based risks while giving comparatively limited attention to conventional military threats. The fact that this remains the case despite Russia's full-scale invasion of Ukraine suggests that NATO is likely to continue to serve as the primary framework for traditional collective defence in Europe.

2 LEGAL ANALYSIS OF ARTICLE 42(7) TEU

Article 42(7) TEU states:

> If a Member State is the victim of armed aggression on its territory, the other Member States shall have towards it an obligation of aid and assistance by all the means in their power, in accordance with Article 51 of the United Nations Charter. This shall not prejudice the specific character of the security and defence policy of certain Member States.
>
> Commitments and cooperation in this area shall be consistent with commitments under the North Atlantic Treaty Organisation, which, for those States which are members of it, remains the foundation of their collective defence and the forum for its implementation.[17]

Several elements seem to deserve further examination:

I. The use of the words 'armed aggression' rather than 'armed attack';

---

of Law in Context 459; William Twinning, Law in Context: Enlarging a Discipline (Oxford University Press, 1997).

[16] Hermann-Josef Blake and Stelio Mangiameli, 'Article 42 [CSDP: Goals and Objectives; Mutual Defence] (ex-Article 17 TEU)' in Hermann-Josef Blake and Stelio Mangiameli (eds), The Treaty on European Union (TEU): A Commentary (Berlin: Springer-Verlag Berlin Heidelberg 2013) 1228.

[17] TEU (n 2) Article 42(7).

II. The fact that the aggression must have taken place on the territory of the aggressed;
III. The framework of response: bilateral (Member States) vs collective (EU);
IV. The phrasing 'obligation of aid and assistance by all the means in their power';
V. The express reference to Article 51 of the Charter of the United Nations (UNC);
VI. The so-called 'Irish formula';
VII. The 'NATO formula'.

1.1 ARMED AGGRESSION VS ARMED ATTACK

An armed attack is a form of armed aggression, which means that armed aggression is a broader category, comprising other forms of aggression beyond armed attacks.[18] Although the two terms are often used interchangeably, some authors[19] have argued that since Article 42(7) TEU refers to armed aggression while Article 5 NAT to armed attack, the former could potentially cover a broader spectrum of threats than the latter.[20] For example, it could be activated for those hybrid acts that do not meet the threshold of armed attack under Article 5 NAT,[21] such as recent incidents in the Baltic Sea.[22] Therefore, at least in theory, EU Member States would be legally bound to collective defence in cases when NATO Allies are not. This argument seems implausible for two reasons.

First, it is not only Article 5 NAT that preferred the coinage armed attack to armed aggression but also Article 51 UNC, which both Article 5 NAT and 42(7) TEU make express

---

[18] See e.g. Federica Fazio, 'Collective defence in NATO: A legal and strategic analysis of Article 5 in light of the war in Ukraine' (5 November 2024) DELI Working Paper Series 2/24, Dublin European Law Institute, 6 <https://zenodo.org/records/14037328> accessed 18 November 2025.

[19] Anne Bakker et al, 'The EU's Mutual Assistance Clause: Spearheading European Defence: Employing the Lisbon Treaty for a Stronger CSDP' (2016) Report, Clingendael, 25 <https://www.jstor.org/stable/resrep05543.8?seq=1> accessed 16 October 2024.

[20] See e.g. Jean-Christophe Martin, 'La Clause de Défense Mutuelle' in Elsa Bernard, Quentin Loïez and Stéphane Rodrigues (eds), L'Union européenne de la défense : commentaire article par article (Bruylant 2024) 408.

[21] As Perot pointed out, 'when it comes to how to react to the most serious forms of hybrid threats, the general idea that emerged […] was that of a division of labor between the EU and NATO, whereby the EU would be responsible for responding first through Article 222 TFEU and then Article 42.7 TEU, while NATO would be called upon to intervene in the event of further escalation, on the basis of its own collective defense clause'. See Elie Perot, 'The European Union's nascent role in the field of collective defense: between deliberate and emergent strategy (2024) 46(1) Journal of European Integration, 11; see also Aurel Sari, 'The Mutual Assistance Clauses of the North Atlantic and EU Treaties: The Challenge of Hybrid Threats' (2019) 10 Harvard National Security Journal 405, 452 and 455. Additionally, Sari has argued that, by covering terrorist attacks and man-made disasters, Article 222 TFEU gives EU Member States legal basis to assist one another in responding to acts of sabotage that fall below the threshold of an armed attack or armed aggression and, therefore, do not trigger Article 5 NAT or Article 42(7) TEU; Ibid 458 and 459.

[22] For an overview of recent incidents in the Baltic Sea, see Reuters, 'Recent suspected underwater sabotage incidents in the Baltic Sea', (21 February 2025), available <https://www.reuters.com/world/europe/recent-suspected-underwater-sabotage-incidents-baltic-sea-2024-12-03/> accessed 15 March 2025; German Federal Foreign Office, 'Joint Declaration by the Foreign Ministers of Germany, France, Poland, Italy, Spain and the United Kingdom in Warsaw' (Press Release, 19 November 2024) <https://www.auswaertiges-amt.de/en/newsroom/news/2685538-2685538> accessed 7 December 2025; European Commission, 'Joint Statement by the European Commission and the High Representative on the Investigation into Damaged Electricity and Data Cables in the Baltic Sea' (Statement, 26 December 2024) <https://ec.europa.eu/commission/presscorner/detail/en/statement_24_6582> accessed 7 January 2025; Statsministeriet, 'Joint Statement of the Baltic Sea NATO Allies', (14 January 2025), available <https://stm.dk/media/ndolltur/joint-statement-of-the-baltic-sea-nato-allies-summit.pdf> accessed 7 January 2025.

reference to.[23] As pointed out by Reichard, Article 103 UNC gives it legal primacy over other international treaties.[24] Article 30(1) of the Vienna Convention on the Law of Treaties (VCLT) reflects the effects of this supremacy.[25] In light of this, and pursuant to the duty of consistent interpretation of EU law with international law – which stems from Articles 3(5) and 21(1) TEU and has been recognised by the Court of Justice of the EU (CJEU) in cases such as *Poulsen* (C-286/90)[26] and *Air Transport Association of America* (C-366/10)[27] – it follows that Article 42(7) TEU should, insofar as possible, be interpreted in conformity with Article 51 UNC. Accordingly, the term 'armed aggression' in Article 42(7) TEU should be understood as synonymous with 'armed attack' under Article 51 UNC.[28]

In the absence of any reference to the motives behind the change in wording from armed attack into armed aggression in the documents that were issued by the European Convention and formalised by the Intergovernmental Conference of the Representatives of the Governments of the Member States between December 2002 and April 2003, it is safe to assume, as some commentators have, that 'the reference to "armed aggression" may simply be the result of a literal translation of the French "agression armée"'.[29]

Second, in 2016, NATO Allies recognised cyberspace as a domain of warfare, alongside land, sea, air and, more recently, space, and countering hybrid threats has been an area of strengthened EU-NATO cooperation ever since.[30] Additionally, '[h]ybrid attacks have been explicitly identified by both the EU Strategic Compass and the NATO Strategic Concept as qualifying for collective response'.[31] Furthermore, earlier this year, NATO announced the launch of Baltic Sentry to bolster its military presence in the Baltic Sea and

---

[23] Fazio, 'Collective defence in NATO' (n 18) 5.
[24] Martin Reichard, 'Collective Self-Defence' in Martin Reichard (ed), The EU-NATO Relationship: A Legal and Political Perspective (Routledge 2006) 210.
[25] See, e.g. Alexander Orakhelashvili, '1969 Vienna Convention. Article 30: Application of Successive Treaties Relating to the Same Subject Matter' in Olivier Corten and Pierre Klein (eds), The Vienna Convention on the Law of Treaties A Commentary (Oxford University Press, 2011) 764 and 780.
[26] Case C-286/90 Poulsen and Diva Navigation EU:C:1992:453 paras 9 and 10.
[27] Case C-366/10 Air Transport Association of America and Others v Secretary of State for Energy and Climate Change EU:C:2011:864 paras 101, 103, and 109.
[28] Blake and Mangiameli (n 16) 122; Martin (n 20) 408-409.
[29] Bob Deen, Dick Zandee, and Adája Stoetman, 'Uncharted and uncomfortable in European defence: The EU's mutual assistance clause of Article 42(7)' (January 2022) Report, Clingendael, 7 <https://www.clingendael.org/sites/default/files/2022-01/uncharted-and-uncomfortable.pdf> accessed 20 September 2024; see also Jolyon Howorth, 'The European Draft Constitutional Treaty and the Future of the European Defence Initiative: A Question of Flexibility' (2004) 9(4) European Affairs Review 483; Elie Perot 'The art of commitments: NATO, the EU, and the interplay between law and politics within Europe's collective defence architecture' (2019) 28(1) European Security 40, 45; Martin (n 20) 408; Sari (n 21) 418.
[30] European Parliament, 'Joint Declaration by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization' (8 July 2016) <https://www.europarl.europa.eu/cmsdata/121580/20160708_160708-joint-NATO-EU-declaration.pdf> accessed 20 September 2024.
[31] Bernard Siman, 'Hybrid Warfare: Attribution is Key to Deterrence' (Egmont Institute, 30 January 2023) <https://www.egmontinstitute.be/hybrid-warfare-attribution-is-key-to-deterrence/> accessed 10 October 2024. Already in 2016, the Joint Framework on countering hybrid threats stated that 'if multiple serious hybrid threats constitute armed aggression against an EU Member State, Article 42 (7) TEU could be invoked to provide an appropriate and timely response. A wide-ranging and serious manifestation of hybrid threats may also require increased cooperation and coordination with NATO'. See European Commission, 'Joint Communication to the European Parliament and the Council-Joint Framework on countering hybrid threats' JOIN(2016) 18 final (6 April 2016)<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52016JC0018> accessed 10 October 2024.

deter further sabotage of critical undersea infrastructure by state and non-state actors alike.[32] Therefore, it seems unreasonable to believe that an act of hybrid warfare would trigger Article 42(7) TEU but not Article 5 NAT.

Article 42(7) traces back to Article 4 of the Brussels Treaty (BT), which, like Article 5 NAT, was originally designed for collective defence against conventional military attacks, not attacks by non-state actors. The article's activation in response to a non-state-sponsored terrorist attack, despite the existence of Article 222 TFEU (which is specifically designed to address such incidents), seems to support the argument of an extensive interpretation of this norm.[33]

Furthermore, like NATO, the EU recognised cyberspace and space as operational domains in 2018[34] and has since put forward a new Cybersecurity Strategy in 2020,[35] a Military Vision and Strategy on Cyberspace as a Domain of Operations in 2021,[36] the first-ever Space Strategy for Security and Defence in 2023,[37] and the Space Act in 2025.[38] As the strategic analysis section will show, there is a strong focus in the Compass on regular exercises to further strengthen mutual assistance in case of armed aggression, particularly in the cyber,[39] hybrid,[40] and space domains.[41] Therefore, it seems safe to assume that, although the interpretation of Article 42(7) TEU has never been discussed or expanded in European Council decisions or conclusions, unlike that of Article 5 NAT in NATO Summit communiqués, Article 42(7) should be considered applicable under the same circumstances as Article 5. Non-traditional attacks, such as terrorist attacks, cyberattacks, hybrid attacks and attacks to, from and within space, are therefore also covered by the EU's Article 42(7), with potential overlaps between the two clauses.[42]

---

[32] NATO, 'Joint Press Conference by NATO Secretary General Mark Rutte with the President of Finland Alexander Stubb and the Prime Minister of Estonia Kristen Michal at the Baltic Sea NATO Allies Summit' (14 January 2025) <https://www.nato.int/cps/en/natohq/opinions_232116.htm> accessed 20 September 2025; SHAPE, 'Baltic Sentry to Enhance NATO's Presence in the Baltic Sea' (14 January 2025) <https://shape.nato.int/news-releases/baltic-sentry-to-enhance-natos-presence-in-the-baltic-sea> accessed 10 February 2025.

[33] Blake and Mangiameli (n 16) 1225-1226; Martin (n 20) 410-411. See also Section 1.3.

[34] Council of the EU, 'EU Cyber Defence Policy Framework' (2018 update) 14413/18 (19 November 2018) <https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/en/pdf> accessed 6 November 2025.

[35] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 'Joint Communication to the European Parliament and the Council - The EU's Cybersecurity Strategy for the Digital Decade' JOIN(2020) 18 final <https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0> accessed 10 October 2025.

[36] European External Action Service, 'European Union Military Vision and Strategy on Cyberspace as a Domain of Operations' EEAS(2021) 706 REV4 <https://www.statewatch.org/media/2879/eu-eeas-military-vision-cyberspace-2021-706-rev4.pdf> accessed 10 October 2025.

[37] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 'Joint Communication to the European Parliament and the Council- European Union Space Strategy For Security and Defence' JOIN(2023) 9 final <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023JC0009> accessed 20 September 2024.

[38] European Commission, Defence Industry and Space, 'EU Space Act: Strengthening Safety, Resilience and Sustainability in Space' (25 June 2025) <https://defence-industry-space.ec.europa.eu/eu-space-act_en> accessed 28 June 2025.

[39] EEAS, 'A Strategic Compass for Security and Defence' (n 4) 31, 35, and 39.

[40] Ibid 31 and 39.

[41] Ibid 34 and 36.

[42] Already in 2012, the European Parliament stated in its resolution on the EU's mutual defence and solidarity clauses: political and operational dimensions that '[…] even non-armed attacks, for instance cyberattacks against critical infrastructure, that are launched with the aim of causing severe damage and disruption to a

1.2 ARMED AGGRESSION ON A MEMBER STATE'S TERRITORY

While Article 5 NAT states that the armed attack against one or more NATO Allies must have been committed in 'Europe or North America', with Article 6 further clarifying the geographical reach of the attack that can trigger the mutual defence obligation, Article 42(7) TEU simply states that a member state must be 'victim of armed aggression on its territory'. This leads to two considerations:

First, only the aggressed Member State(s) can invoke Article 42(7) TEU. It was France, the victim of the terrorist attacks, that invoked Article 42(7) in 2015. In contrast, in the case of Article 5 NAT, it was not the US, the victim of the terrorist attack, but its Allies who offered to invoke it.[43]

Second, in light of the fact that no further clarification is provided in terms of geographical coverage, overseas territories outside of Europe should be intended as included in the scope of Article 42(7). For example, should an attack occur on the land, in the waters or in the airspace of the French territory of *La Martinique*, in the Caribbean, France could potentially invoke Article 42(7) as it did after the Paris attacks. It could not invoke NATO's Article 5 though, since the island is located below the Tropic of Cancer.[44]

However, it has been argued that since EU primary law does not apply to all overseas territories, neither should Article 42(7) TEU.[45] In fact, some scholars and practitioners[46] have analysed the distinction between the EU's outermost regions (ORs), which include for example *La Martinique*, and the EU's overseas countries and territories (OCTs).

The former are part of EU territory, subject to EU law, and enjoy all the rights and obligations of EU membership, though certain specific measures apply.[47] In contrast, the latter are associated with the EU but not considered part of it.[48] While EU law does not extend to them, their foreign, security and defence policy often falls under the jurisdiction of

---

Member State and are identified as coming from an external entity could qualify for being covered by the clause'. See European Parliament, 'European Parliament resolution of 22 November 2012 on the EU's mutual defence and solidarity clauses: political and operational dimension (2012/2223(INI))' P7 TA(2012)0456 para 13 <https://www.europarl.europa.eu/doceo/document/TA-7-2012-0456_EN.pdf> accessed 5 September 2024. As observed by Martin, following the Bataclan and Stade de France attacks, however, the EEAS further clarified that, to fall within the scope of Article 42(7) TEU and constitute armed aggression, 'The attack must originate from abroad and its scope covers attacks by state and non-state actors [translated from French]', as quoted in Martin (n 20) 410-411; see also Sari (n 21) 422.

[43] Fazio, 'Collective defence in NATO' (n 188) 6.

[44] Pol Navarro I Serradell, A Comparative Study of Article 5 of the NATO and Article 42(7) of the Treaty on the European Union: Its Scope and Limits (Finabel 2024) 12.

[45] Blake and Mangiameli (n 16) 1226; see also Carmen-Cristina Cirlig, 'The EU's mutual assistance clause. First ever activation of Article 42(7) TEU' (Briefing, European Parliamentary Research Service, 27 November 2015), 3 <https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2015)572799> accessed 10 November 2024.

[46] See, e.g., Perot, 'The art of commitments' (n 29) 49; Deen et al (n 29) 17; Wessel Willem Geursen, Mapping the territorial scope of EU law (PhD thesis, Vrije Universiteit Amsterdam 2024) <https://research.vu.nl/ws/portalfiles/portal/307385687/ww%20geursenmapping%20the%20territorial%20scope%20of%20eu%20lawthesis%20including%20annexes%20-%2065e4818190907.pdf> accessed 18 February 2025.

[47] Consolidated Version of the Treaty on the Functioning of the European Union [2016] OJ C202/195, 197, Articles 349 and 355. ORs are currently 9 in total. For the full list see <https://ec.europa.eu/regional_policy/policy/themes/outermost-regions_en> accessed 20 September 2024.

[48] Although some researchers believe otherwise; see, e.g., Geursen (n 46) 148; TFEU Articles 198-204. OCTs are currently 13. The full list can be found at <https://international-partnerships.ec.europa.eu/countries/overseas-countries-and-territories_en> accessed 20 September 2024.

the EU Member States they maintain special ties with. As EU law applies to ORs but not OCTs, it follows that Article 42(7) TEU could be invoked for ORs but not for OCTs.[49] This classification has gained renewed attention following US President Donald Trump's refusal to rule out the use of military force to acquire Greenland, an OCT.[50]

However, the status of ORs and OCTs can be easily changed by the European Council without requiring any amendment to the TFEU. The French territory of Mayotte, for example, was originally an OCT until 2014 when it became an OR at the request of France.[51] Were it to come under attack, France could, therefore, invoke Article 42(7). This also applies to the Spanish cities of Ceuta and Melilla in Morocco,[52] which, although located above the Tropic of Cancer, are not covered by Article 5 NAT.[53]

As Sari has pointed out, unlike Article 5 NAT, Article 42(7) cannot be invoked if the armed forces of a Member States are attacked while deployed in the territory of another Member State.[54] The clause's sole reference to Member State territories also appears to exclude its applicability to ships in international waters or military personnel deployed out of area. This means that, if vessels flying an EU Member State's flag are attacked in international waters, or if soldiers participating in a CSDP mission or other external operation come under attack, Article 42(7) TEU does not apply.[55] As such, the French proposal earlier this year to send European troops – outside of NATO and without US support – to help secure a potential ceasefire between Russia and Ukraine would have left them vulnerable to aggression. This consideration is likely among the factors that prompted the President of the European Commission, Ursula von der Leyen, to negotiate with President Trump a multinational troop deployment with US backing as part of post-conflict security guarantees to Ukraine.[56]

The same logic seems to extend to outer space. As pointed out by Fiott,[57] it is not clear whether Article 42(7) TEU applies to space-based assets and personnel. Under international

---

[49] Although Perot suggests that the fact that OCTs are not part of the EU does not preclude an armed aggression there from triggering the obligation of aid and assistance among EU Member States under Article 42(7) TEU, while Geursen argues that CFSP legislation should apply uniformly to all overseas territories, and that allowing a division in its application would undermine its coherence. See Perot, 'The art of commitments' (n 29) 49; Geursen (n 46) 148.

[50] See, e.g., Federica Fazio, 'What happens if Trump invades Greenland?' (DCU Brexit Institute, 13 January 2025) <https://dcubrexitinstitute.eu/2025/01/what-happens-if-trump-invades-greenland/> accessed 14 January 2025.

[51] Frédéric Gouardères, 'Outermost regions (ORs)' (Fact Sheet on the European Union, European Parliament, March 2024) <https://www.europarl.europa.eu/factsheets/en/sheet/100/outermost-regions-ors> accessed 20 September 2024.

[52] For more information on EU territories, see <https://taxation-customs.ec.europa.eu/territorial-status-eu-countries-and-certain-territories_en> accessed 20 September 2025.

[53] Serradell (n 44) 12.

[54] Sari (n 21) 455.

[55] Perot, 'The art of commitments' (n 29) 50; Deen et al (n 29) 18.

[56] Henry Foy, 'Europe has 'pretty precise' plan to send troops to Ukraine, von der Leyen says', (Financial Times, 31 August 2025), available <https://www.ft.com/content/8ade14ca-7aa1-4413-887b-59712037665c> accessed 6 September 2025; see also Delegation of the European Union to Ukraine, 'Statement by President von der Leyen following the meeting of the Coalition of the Willing in Paris', Paris, (5 September 2025), available <https://www.eeas.europa.eu/delegations/ukraine/statement-president-von-der-leyen-following-meeting-coalition-willing-paris_en> accessed 6 September 2025.

[57] Daniel Fiott, 'The Strategic Compass and EU space-based defence capabilities' (In-Depth Analysis Requested by the SEDE Sub-Committee, European Parliament, November 2022), 26-27 <https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702569/EXPO_IDA(2022)702569_EN.pdf> accessed 30 September 2024.

law, sovereignty cannot be asserted in space. The 1967 Outer Space Treaty – to which all EU Member States are now parties[58] – affirms that '[o]uter space, including the Moon and other celestial bodies, is not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means'.[59] Therefore, Article 42(7) TEU could apply in the event of an attack originating from space and targeting the territory of a Member State, but not, for example, to attacks on EU astronauts aboard the International Space Station or on satellite systems such as Copernicus or Galileo, unless the attack coincides with their orbiting directly above a Member State's territory. Nevertheless, the 2023 EU Space Strategy for Security and Defence, clearly states that '[a]ny Member State can invoke the mutual assistance clause enshrined in the EU Treaties (Article 42(7) of the Treaty on European Union), *should a space threat or incident amount to an armed attack on its territory*'.[60] This was followed by amendments to Council Decision (CFSP) 2021/698,[61] to extend its scope to threats in the space domain that may affect the security of the EU and its Member States, and particularly those to the systems and services set up under the Union Secure Connectivity Programme. More recently, the European Commission proposed the EU Space Act, aimed at strengthening protection of European space infrastructure by extending cybersecurity regulations to the space sector.[62] These developments suggest a broader interpretation of Article 42(7) TEU, potentially encompassing attacks from, to, or even within space, provided they are considered an armed attack on a Member State's territory.[63]

1.3 FRAMEWORK OF RESPONSE: BILATERAL (MEMBER STATES) VS COLLECTIVE (EU) RESPONSE

While Article 42(7) TEU commits only the Member States to come to each other's assistance in case of armed aggression, another norm, Article 222 TFEU, requires both the Member States and the EU institutions to provide support in the event of terrorist attacks as well as man-made or natural disasters.[64]

The solidarity clause was first introduced into the EU legal framework during the negotiations leading to the signing of the Constitutional Treaty (CT), as was the mutual defence clause. In the final version of the CT signed on 29 October 2004, the solidarity clause and its implementation mechanism were indicated in Article I-43 and Article III-329,

[58] Croatia acceded in March 2023 while Latvia in March 2025. For more information see <https://hina.hr/news/11151003> and <https://www2.mfa.gov.lv/en/vienna/news/72300-latvia-officially-joins-the-outer-space-treaty> accessed 20 April 2025.
[59] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and other Celestial Bodies (27 January 1967), 610 UNTS 205, Article 2.
[60] Joint Communication to the European Parliament and the Council- European Union Space Strategy For Security and Defence (n 37) 9, emphasis added.
[61] See Council of the EU, 'Council Decision (CFSP) 2023/598 of 14 March 2023 amending Decision (CFSP) 2021/698 to include the Union Secure Connectivity Programme' [2023] OJ L79/165.
[62] European Commission, 'Commission proposes EU Space Act to boost market access and strengthen space safety' (Press Release, 25 June 2025) <https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1583> accessed 18 July 2025.
[63] See Martin (n 20) 407-408.
[64] TFEU n (47) Article 222

respectively.[65] Then, when the CT project failed, the solidarity clause made its way first into the Lisbon Treaty (LT) as Article 188 R, which merged Article I-43 and Article III-329,[66] and eventually into the TFEU as Article 222. Declaration 37 on Article 222 TFEU reiterated what stated in Declaration 9 on Article I-43 and III-329, which is that this legal provision was not 'intended to affect the right of another Member State to choose the most appropriate means to comply with its own solidarity obligation'.[67] This suggests that, akin to the mutual defence clause, the solidarity clause may be understood as an *obligation of result rather than means*, notwithstanding the fact that, unlike the former, it makes express reference to military assistance.[68] Although neither Article 42(7) TEU nor Article 222(1) (b) TFEU expressly defines the specific outcome toward which the assistance must be directed – whereas Article 5 NAT explicitly frames collective action in terms of 'restoring and maintaining the security of the North Atlantic area' – their underlying purpose may nonetheless be inferred. In particular, Article 3(1) TEU affirms that '[t]he Union's aim is to promote peace, its values and the well-being of its peoples', which, as Govaere has emphasised, constitutes 'the first (and foremost) express objective of the EU'.[69] Read together, these provisions arguably support the view that the commitments under Article 42(7) TEU and 222 TFEU entail 'internal' obligations of result.[70]

Given that the intent of the legislator was for the solidarity clause to cover terrorist attacks by non-state actors,[71] France should have invoked Article 222 TFEU, the solidarity clause, rather than Article 42(7) TEU, the mutual assistance clause, after the attacks by the Islamic State or Iraq and Syria (ISIS) that killed 131 people and injured 416 in Paris on 13 November 2015. However, the French government chose to invoke Article 42(7) TEU for three reasons: (1) Article 42(7) TEU involves only Member States, with no formal role for the EU as such; (2) invoking it does not require a unanimous decision by the Council; and (3) there is no formal procedure to be followed to activate it.

Article 222 TFEU, on the other hand, explicitly refers to the role the EU would play if invoked, which is to mobilise all available instruments, including the military resources provided by the Member States.[72] Additionally, paragraph 3 states that where its decisions have defence implications, the Council needs to act in accordance with Article 31(1) TEU, which requires decisions to be taken by unanimity, save for the possibility of constructive abstention.

---

[65] 'Treaty establishing a Constitution for Europe' (2024) CIG 87/2/04 REV 2, Article I-43 and Article III-329 <https://data.consilium.europa.eu/doc/document/CG%2087%202004%20REV%202/EN/pdf> accessed 20 September 2024.
[66] 'Treaty of Lisbon' [2007] OJ C 306/1, Article 188 R.
[67] Declaration 37 on Article 222 (n 47).
[68] As pointed out by Cirlig, however, 'the Council Decision [2014/415/EU] does not represent a legal framework for action if military means are used for defence purposes' since it specifically states that it has no defence implications; see Cirlig (n 45) 7. For more information on Council Decision 2014/415/EU see n 73.
[69] Inge Govaere, 'Transformative Impact on the European Union of War (in Ukraine): Existential Conundrums', in Inge Govaere, Sacha Garben and Eleanor Spaventa (eds.) The Impact of War (in Ukraine) on the EU. (Oxford and Dublin: Hart Publishing, 2025) 13.
[70] TEU (n 2) Article 3(1); Inge Govaere, 'Promoting the Rule of Law in EU External Relations: A Conceptual Framework', 03(22) Research Paper in Law, Department of European Legal Studies, College of Europe (2022) 4.
[71] Deen et al (n 29) 10-11; Tom Dyson and Theodore Konstadinides 'The Legal Underpinnings of European Defense Cooperation' in Tom Dyson and Theodore Konstadinides (eds), European Defense Cooperation in EU Law and IR Theory (Palgrave Macmillan, 2013) 69.
[72] Deen et al (n 29) 10-11.

The exact procedure for the implementation of Article 222 TFEU by the Union is set out in the Council Decision of 24 June 2014. The Decision not only further clarifies what is meant by terrorist attack,[73] but also poses a condition on the invocation of the clause: 'the affected Member State may invoke the solidarity clause *if, after having exploited the possibilities offered by existing means and tools at national and Union level, it considers that the crisis clearly overwhelms the response capabilities available to it*'.[74]

By contrast, no formal procedure is foreseen for the implementation of Article 42(7) TEU, making this norm more flexible. When former French Minister of Defence, Jean-Yves Le Drian, formally invoked Article 42(7) TEU at a meeting of the EU Foreign Affairs Council (FAC) on 17 November 2015, the Ministers of Defence of the then-28 Member States expressed their 'unanimous and full support to France and their readiness to provide all the necessary aid and assistance'.[75] However, the FAC meeting had already been scheduled,[76] and simply provided the opportunity for Le Drian to invoke the clause while his counterparts were already assembled. The clause's invocation in a Council's meeting was, therefore, 'purely incidental'.[77] Yet, the meeting could also be interpreted as an implementation of Article 32 TEU, which in a similar vein to Article 4 NAT, states that 'Member States shall consult one another within the European Council and the Council on any matter of foreign and security policy of general interest, in order to determine a common approach'.[78]

Former High Representative for Foreign Affairs and Security Policy, Federica Mogherini, clarified that this assistance would consist in 'offers of support through material assistance as well as through enhanced support in other theatres [of operations where France was engaged], and that 'the article of the Treaty does not require any formal decision or

---

[73] 2014/415/EU: Council Decision of 24 June 2014 on the arrangements for the implementation by the Union of the solidarity clause Article 3 [2014] OJ L192/55. The Council Framework Decision 2002/475/JHA is no longer in force as it was replaced by Directive 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism. For the full list of acts that constitute terrorist offences, see Title II, Directive (EU) 2017/541 Article 3 [2017] OJ L 88/6 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA. Council Decision 2014/415/EU Article 3 also defines a member state's territory for these purposes to include not only its 'land area, internal waters, territorial sea, and airspace', but also 'infrastructure (such as off-shore oil and gas installations)', located in its territorial sea, exclusive economic zone, or continental shelf.

[74] Ibid Article 4, emphasis added.

[75] Council of the EU, 'Outcome of the Council Meeting. 3426th Council meeting, Foreign Affairs, 14120/15' (Presse 69, PR CO 61, 16 and 17 November 2015), 6, <https://www.consilium.europa.eu/media/23101/st14120en15.pdf> accessed 6 September 2024.

[76] European Commission, 'LIVE Foreign Affairs Council (Defence) – press conference HRVP Federica Mogherini' (17 November 2015), at 9:10 <https://audiovisual.ec.europa.eu/en/video/I-112324> accessed 10 October 2024.

[77] Christophe Hillion and Steven Blockmans, 'Europe's self-defence: Tous pour un et un pour tous?' (CEPS Commentary, Centre for European Policy Studies, 20 November 2015), 3 <https://cdn.ceps.eu/wp-content/uploads/2015/11/CH%20&%20SB%20Tous%20pour%20un%20CEPS%20Commentary_0.pdf> accessed 10 0ctober 2025; see also Cirlig (n 45) 5.

[78] TEU (n 2) Article 32. See e.g. Martin (n 20) 417. As a matter of fact, in 2012 the European Parliament had expressed the view that '[…] the obligation to provide aid and assistance, expressing political solidarity among Member States, should ensure a rapid decision in Council in support of the Member State under attack; considers that consultations in line with the requirement of Article 32 TEU would serve this purpose, without prejudice to the right of each Member State to provide for its self-defence in the meantime'. See European Parliament resolution of 22 November 2012 on the EU's mutual defence and solidarity clauses (n 42) para 17; see also Sari (n 21) 436.

Council conclusion to be taken'.[79] No decision was in fact adopted by the Council. The obligations imposed by Article 42(7) TEU, therefore, unlike those under Article 222 TFEU and Article 5 NAT, are in theory *automatic*, despite the shift in verb tense from 'will' in Article 5 BT to 'shall' in Article 42.7 LT.[80] Mogherini also clarified that 'this doesn't imply EU CSDP mission or operation'.[81]

At a joint press conference with Mr Le Drian on 17 November, Ms Mogherini added that, although the process would be *Member State-driven* and the aid and assistance provided bilaterally, 'the European Union c[ould] facilitate this and coordinate this' if useful and necessary.[82] Therefore, although the article does not formally envision a role for EU institutions, the attacked Member State can still request the EU's support, for instance when it comes to coordinating the overall aid and assistance, as France did.[83]

Following the activation of the mutual assistance clause, bilateral negotiations took place between Member States and the French government regarding the type of aid to be provided. Le Drian specifically requested that the assistance take the form of support for France in external theatres of operations, particularly in Mali, the Sahel, Iraq and Syria.[84] As Mogherini had anticipated, the assistance differed based on the foreign and defence policies of each Member State.[85] For instance, Ireland increased its personnel assigned to the EU Training Mission in Mali, which had been established in 2013 to support French operations against militant Islamist groups in Mali and the Sahel region through Operations

---

[79] Press Conference HRVP Federica Mogherini (n 76) at 3:24, and 4:01.
[80] Cirlig (n 45) 3.
[81] Press Conference HRVP Federica Mogherini (n 76) at 4.15. As highlighted by Cirlig, 'in principle, the EU cannot conduct self-defence operations within the framework of the CSDP (only its Member States), unless the Treaty is amended or the European Council decides unanimously on the establishment of common defence in accordance with Article 42(2) TEU'. See Cirlig (n 45) 4.
[82] Press Conference HRVP Federica Mogherini (n 76) at 4:25.
[83] Already in 2012, in its resolution on the 'EU mutual defence and solidarity clauses: political and operational dimensions', the European Parliament had invited the HR/VP 'to propose practical arrangements and guidelines for ensuring an effective response in the event that a Member State invokes the mutual defence clause, as well as an analysis of the role of the EU institutions should that clause be invoked'. European Parliament resolution of 22 November 2012 on the EU's mutual defence and solidarity clauses (n 42) para 17. Although these calls were reiterated in 2016, no procedural framework appears to have been established at the time of writing. An 'operational protocol' was adopted a few months later, but it addressed only the eventuality of hybrid attacks and referred exclusively to Article 222 TFEU, not Article 42(7) TEU, even though the subsequent implementation report expressly mentions both articles. Additionally, in 2012, the European Parliament had also expressed the view that '[…] where collective action is taken to defend a Member State under attack, it should be possible to make use of existing EU crisis management structures where appropriate, and in particular that the possibility of activating an EU Operational Headquarters should be envisaged; stresses that a fully-fledged permanent EU Operational Headquarters is needed […]'. See European Parliament, 'Resolution on the mutual defence clause (Article 42(7) TEU) (2015/3034(RSP))' P8_TA(2016)0019 paras 17-18 <https://www.europarl.europa.eu/doceo/document/TA-8-2016-0019_EN.pdf> accessed 14 October 2024; see also Council of the EU, 'Joint Staff Working Document EU operational protocol for countering hybrid threats "EU Playbook"' 11034/16 (7 July 2016) <https://www.statewatch.org/media/documents/news/2016/jul/eu-com-countering-hybrid-threats-playbook-swd-227-16.pdf> accessed 14 October 2024; European Commission, 'Joint Report to the European Parliament, the European Council and the Council on the implementation of the Joint Framework on countering hybrid threats from July 2017 to June 2018' JOIN(2018) 14 final <https://www.eeas.europa.eu/sites/default/files/joint_report_on_the_implementation_of_the_joint_framework_on_countering_hybrid_threats_from_july_2017_to_june_2018.pdf> accessed 14 October 2024; see also Cirlig (n 45) 9; Martin (n 20) 421; Perot, 'The European Union's nascent role in the field of collective defense' (n 21) 7.
[84] Press Conference HRVP Federica Mogherini (n 76) at 08:32.
[85] Ibid at 4:55.

Serval and Barkhane.[86] The next section will show that the aid provided can, in fact, include both civil and military assistance, as the clause imposes *an obligation of result but not means*.

1.4 OBLIGATION OF AID AND ASSISTANCE BY ALL THE MEANS IN THEIR POWER

As pointed out by Mills, Article 42(7) TEU is a compromise norm between 'those seeking a mutual defence commitment […], those seeking to protect their traditional neutral status […and] those wanting to ensure that the article would not undermine NATO'.[87] This is reflected, first of all, in the kind of aid and assistance that EU Member States are legally obliged to provide under Article 42(7). The wording '*by all the means in their power*' seems to suggest that the assistance offered can be either civil or military in kind, depending on the means Member States have at their disposal and the nature and gravity of the armed aggression.[88] An explicit reference to military means appeared in Article 4 BT and later Article 5 of the Modified Brussels Treaty (MBT), but was then abandoned in draft Article I-40(7) CT. Despite this, the fact that there is no expressed exclusion seems to imply that the type of aid and assistance that the Member States are compelled to provide could potentially also include military means.[89]

The article's placement in Section 2, under the Provisions on the Security and Defence Policy, strongly supports this interpretation.[90] This argument is further reinforced by the inclusion of the Irish and NATO clauses that follow, as their presence would be unnecessary if military means were not contemplated. Moreover, unlike the phrasing 'as it deems necessary' in Article 5 NAT, which grants Allies discretion over the nature, timing, and scale of their response,[91] the wording 'by all the means in their power' in Article 42(7) TEU appears to allow far less flexibility.[92] This has led some authors to argue that, unlike Article 5 NAT, Article 42(7) TEU 'entails an *unconditional obligation* of mutual assistance'.[93] Yet, the presence of the Irish and NATO clauses does pose conditions, as will be analysed in Sections 1.6 and

---

[86] House of the Oireachtas, 'EU Issues - Dáil Éireann Debate - Written answers by the Irish Minister for Foreign Affairs and Trade Charles Flanagan' (27 September 2016) <https://www.oireachtas.ie/en/debates/question/2016-09-27/467/> accessed 14 October 2024. For information on the other Member States, see, e.g. Cirlig (n 45) 6; see also Suzana Elena Anghel and Carmen-Cristina Cirlig, 'Activation of Article 42(7) TEU: France's request for assistance and Member States' responses' (Briefing, European Parliamentary Research Service, December 2015), 2 <https://www.europarl.europa.eu/EPRS/EPRS-Briefing-573883-Activation-of-article-42-7-FINAL.pdf> accessed 20 September 2024.

[87] Claire Mills, 'France and Article 42(7) of the Treaty on the European Union' (Briefing Paper 7390, House of Commons, 18 November 2015), 3 <https://researchbriefings.files.parliament.uk/documents/CBP-7390/CBP-7390.pdf> accessed 20 September 2024; see also Cirlig (n 45) 2.

[88] Sari (n 21) 434-435.

[89] Reichard (n 24) 201; Cirlig (n 45) 3; Perot, 'The art of commitments' (n 29) 53; Martin (n 20) 417-418.

[90] Hillion & Blockmans, and Martin have argued that for this reason it is not excluded that the provision of aid and assistance could also take the form of a CSDP mission or operation. See Hillion and Blockmans (n 77) 3; Martin (n 20) 420. Mogherini, however, excluded it when France invoked the clause in 2015.

[91] Fazio, 'Collective defence in NATO' (n 18) 8-9.

[92] Martin (n 20) 418-419; Sari (n 21) 438. The German Federal Court, however, clearly affirmed that the EU's collective defence clause does not go beyond NATO's collective defence clause. See German Federal Constitutional Court, Judgment on the Treaty of Lisbon (30 June 2009) para 386 <https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2009/06/es20090630_2bve000208en.html> accessed 20 January 2025.

[93] Blake and Mangiameli (n 16) 1228.

1.7. Therefore, much like NATO Allies, EU Member States are free to choose the type and scope of assistance.

1.5 THE EXPRESS REFERENCE TO ARTICLE 51 OF THE UNITED NATIONS CHARTER

Like Article 5 NAT, Article 42(7) TEU makes express reference to Article 51 UNC. This reference was first introduced in Article 4 BT, and kept in Article 5 MBT and Article I-41(7) CT. This is because Article 51 UNC allows the members of the international community to act in both individual and collective self-defence in case of an armed attack directed against one of them, without previous authorisation by the UN Security Council. Both Article 5 NAT and Article 42(7) TEU are expressions of the right of collective defence and, therefore, the obligations they envisage must be consistent with Article 51 UNC.[94]

1.6 THE IRISH CLAUSE

This clause did not form part of either Article 4 BT or Article 5 MBT. It first appeared in the Maastricht Treaty,[95] primarily in response to Ireland's concerns about neutrality, and later made its way into the collective defence clause with the draft CT and later the LT.[96] The provision is generally understood to refer to militarily non-aligned Member States and countries with long-standing traditions of neutrality – currently Austria, Cyprus, Ireland and Malta – or special security and defence arrangements – such as those with Denmark, which until 2022 had an opt-out from the CSDP.[97] The clause no longer applies to Finland and Sweden, which joined NATO in 2023 and 2024, respectively.

These 'special status' countries are not required to disregard their positions to comply with mutual defence obligations. According to Sari, only these Member States are entitled to decline to provide military assistance when the gravity of the situation would call for a military response.[98] However, Article 42(7) TEU does not clearly state which countries are covered by this clause and, this is something that cannot be determined without looking at the drafting history of the article.[99] According to some scholars, the clause could potentially apply also to Member States like Germany, where parliamentary authorisation of the use of force is constitutionally required.[100] As Martin suggested, if a Member States' parliament

---

[94] An in-depth analysis and discussion of collective defence in international law is outside the scope of this article. A brief overview is, however, essential to understand EU Member States' collective defence obligations and how they relate to UN principles.
[95] Article lJ.4(4)(n 3).
[96] Protocol on the concerns of the Irish people on the Treaty of Lisbon [2013] OJ L60/132 Article 3.
[97] Council of the EU, 'EU defence cooperation: Council welcomes Denmark into PESCO and launches the 5th wave of new PESCO projects' (Press Release, 23 May 2023), <https://www.consilium.europa.eu/en/press/press-releases/2023/05/23/eu-defence-cooperation-council-welcomes-denmark-into-pesco-and-launches-the-5th-wave-of-new-pesco-projects/> accessed 4 October 2024.
[98] Sari (n 21) 435.
[99] Reichard (n 24) 211; Martin (n 20) 419.
[100] Cirlig (n 45) 4; Perot, 'The art of commitments' (n 29) 52; Martin (n 20) 419. The UK as well, at the time. As reported by Mills, 'The Government ha[d] stated its intention to seek the approval of the House before committing military forces to action against ISIS in Syria. However, France's invocation of a treaty obligation ha[d] raised questions among many observers as to whether a treaty obligation represents a critical national

refuses to authorise the use of military force such a legal obstacle would exclude the State's participation in military operations without it being considered in breach of the obligation to provide aid and assistance under Article 42(7) TEU.[101] This confirms that the obligations arising under Article 42(7) TEU may be better understood as obligations of result rather than of means. In the case of an obligation of result, a state is generally presumed to be in breach if the envisaged outcome is not achieved, unless it can invoke a lawful excuse. By contrast, an obligation of means requires that a state undertakes appropriate and reasonable efforts, irrespective of whether the intended outcome is ultimately attained.

The EU's collective defence clause seemingly suggests that various degrees of commitment were envisioned for each member state based on the unique nature of their respective security and defence policies. Yet, this would translate in an evident asymmetry in military obligations, undermining the core purpose of the mutual defence clause, which is to ensure an equal sense of security among all parties involved.[102] The fact that Ireland – and initially Germany, which now also provides lethal assistance – have, through the EPF, provided non-lethal military support to Ukraine, which is not an EU Member State but a candidate country, in the context of Russia's war of aggression, suggests that this category of Member States would not be completely exonerated from the legal obligation to provide aid and assistance in the event of an invocation of Article 42(7) TEU; rather, they would be entitled to choose means of assistance which are not incompatible with their status or domestic law requirements.[103] This contrasts with the argument that Member States are called 'to examine on a case-by-case basis whether their status requires non-participation' with the conclusion varying depending on the country.[104]

However, it should be noted that the CJEU has, in principle, no jurisdiction on CFSP and CSDP, and, therefore, Article 42(7) TEU.[105] The CJEU only has jurisdiction over Article 222 TFEU.[106] Therefore, as with NATO, if any Member State, whether or not it falls within the aforementioned category, decides to provide little or no aid and assistance at all, there is no sanctioning mechanism to compel it to act otherwise.[107]

1.7 THE NATO CLAUSE

The 'NATO clause', like the Irish clause, was not included in Article 5 MBT but was later incorporated into Article I-41(7) CT. Based on this clause, special caveats also apply to the 23 EU Members States that are members of NATO. This seems to imply that, for

interest and, therefore, whether prior parliamentary approval would now need to be sought for expanding UK military operations against ISIS'. See Mills (n 87) 4-5.

[101] Martin (n 20) 419.

[102] Reichard (n 24) 211; Blake and Mangiameli (n 16) 1228-1229.

[103] House of the Oireachtas, 'Ukraine War Dáil Éireann Debate' (8 May 2024) <https://www.oireachtas.ie/en/debates/question/2024-05-08/74/> accessed 20 September 2024; German Federal Government, 'The arms and military equipment Germany is sending to Ukraine' (19 August 2024) <https://www.bundesregierung.de/breg-en/news/military-support-ukraine-2054992> accessed 20 September 2024; see also Cirlig (n 45) 4; Martin (n 20) 416.

[104] Blake and Mangiameli (n 16) 1229; see also Dyson & Konstadinides (n 71) 69.

[105] TEU (n 2) Article 24(1); and TFEU (n 47) Article 275; see also Panos Koutrakos, 'Judicial Review in the EU's Common Foreign and Security Policy' (2018) 67(1) International and Comparative Law Quarterly 1.

[106] Cirlig (n 45) 7; Sari (n 21) 425.

[107] Fazio, 'Collective defence in NATO' (n 18) 9.

members of both organisations, mutual defence obligations arising from the NAT have primacy over those arising from the TEU.[108] This is consistent with Article 8 NAT,[109] as well as Article 30(2) VCLT.[110]

Therefore, the EU's mutual defence obligation would only apply as long as it did not conflict with the prevailing obligation under the NAT.[111] For this reason, before its invocation in 2015, it was thought that the EU's mutual defence clause could only be triggered for attacks against non-NATO EU Member States.[112] The French case has shown, however, that, in the event of an attack, members of both organisations can choose which of the two articles to invoke. It has also revealed that calling for one does not automatically trigger the other, though this does not preclude the possibility of simultaneously invoking both clauses if necessary.[113] As highlighted by Fiott, 'such a situation would raise chain of command, financing and transportation considerations'.[114]

The article could also potentially be invoked by a non-NATO EU Member State against a non-EU NATO Ally, unlike Article 5 MBT.[115] In hypothesis, if attacked, Cyprus – or Greece which is in NATO, however – could, for example, activate the EU's collective defence clause against Turkey.[116] As a matter of fact, in 2020 Greece and Turkey were on the verge of war in the Eastern Mediterranean and, at one point, the Greek government made express reference to Article 42(7) TEU.[117] In such a scenario, members of both organisations could be subject to competing requests for assistance as they have only one set forces. Therefore, NATO obligations would probably take precedence over European

---

[108] Blake and Mangiameli (n 16) 1217.
[109] North Atlantic Treaty, 4 April 1949, 63 Stat. 2241, 34 UNTS 243, Article 8.
[110] Vienna Convention on the Law of Treaties, 22 May 1969, 1155 UNTS 331, Article 30(2).
[111] As Sari has pointed out, this, however, is not the case for Article 222 TFEU. He argues that if a terrorist attack or a man-made disaster rises to the level of an armed attack or aggression, the solidarity clause could apply in parallel with the EU and NATO's mutual defence clauses. In such cases, however, military assistance provided under Article 222 is not subject to the requirement that it be compatible with commitments undertaken within NATO. See Sari (n 21) 439.
[112] Reichard (n 24) 221.
[113] Sari (n 2121) 425 and 435; Bakker et al (n 19) 26; Daniel Fiott, 'Rising Risks: Protecting Europe with the Strategic Compass' (CSDS Policy Brief 10/2022, Centre for Security, Diplomacy and Strategy, 12 May 2022), 2 <https://csds.vub.be/publication/rising-risks-protecting-europe-with-the-strategic-compass/> accessed 20 September 2024.
[114] Fiott, 'Rising Risks' (n 113) 3.
[115] The 2003 Berlin Plus framework agreement consists of classified letter exchanges between then-EU High representative Javier Solana and then-NATO Secretary General Lord Robertson. In one such letter, Solana allegedly stated that the ESDP and, therefore, also the EU's mutual defence clause, would never be used against a NATO Ally. However, as Reichard noted, the Berlin Plus arrangements are not binding. Reichard (n 24) 222.
[116] Since Cyprus joined the EU in 2004, formal cooperation between the two institutions has stalled due to the unresolved dispute between Turkey, a non-EU NATO Ally, and Cyprus, a non-NATO EU Member State, over the latter's sovereignty. Twenty years later, seemingly insurmountable obstacles still stand in the way of a peace deal and the two countries keep using their respective leverage, Turkey within NATO and Cyprus within the EU, to prevent formal meetings between the two institutions, blocking formal cooperation. For more information, see, e.g., Simon J Smith and Carmen Gebhard, 'EU–NATO relations: running on the fumes of informed deconfliction' (2017) 26(3) European Security 303.
[117] Deen et al (n 29) 41-42; see also Elie Perot, 'Solidarity and Deterrence in the Eastern Mediterranean: An Analysis of the Delicate Question of Collective Defence Between EU Member States Vis-à-Vis Turkey' (13/2021 Fondation pour la recherche stratégique (FRS), June 2021), 11-12 <https://www.frstrategie.org/sites/default/files/documents/publications/recherches-et-documents/2021/132021.pdf> accessed 16 June 2025.

obligations.[118] Still, whether this precedence would truly apply also depends on the circumstances of the clause's invocation.[119]

Additionally, this primacy of NATO over EU commitments does not amount to a 'right of first refusal' in favour of NATO. Despite the fact that the 2003 Berlin Plus arrangements did include a right of first refusal for NATO, even for peacekeeping operations, the launch of Operation Artemis in the Democratic Republic of Congo in June 2003 made it very clear that this was not the case.[120] The 1999 Helsinki European Council Conclusions had stated that the EU would act only in instances 'where NATO as a whole is not engaged',[121] but as pointed out by Blake & Mangiameli, 'this principle is a matter of policy and not of law and in no way means that the EU may only act when NATO has refused to implement a special operation'.[122] The two organisations have, in fact, conducted parallel operations in the same geographical areas, such as in Kosovo, Afghanistan and the Horn of Africa.

Finally, Reichard noted that, were a non-NATO EU Member State to be attacked, it could benefit from NATO's mutual security guarantee 'through the back door'.[123] Indeed, were Ireland to be attacked, for example, it is hard to imagine that the US and the UK would refrain from intervening or impose missile restrictions; or at least it was hard to imagine before Trump returned to the White House.

2 STRATEGIC ANALYSIS

'Mutual assistance clauses serve a dual purpose. They commit their signatories to stand up to a common threat and are thereby meant to deter potential aggressors. Their dual purpose places them at the crossroads between war and peace and the intersection between law and strategy'.[124] With this dual role in mind, this Section analyses the 2016 EUGS and the 2022 Strategic Compass, as well as their related implementation strategies and progress reports. The strategic analysis reveals that, despite the EU's growing role in defence, the Union places greater emphasis on unconventional threats – such as terrorism, cyber, hybrid, and space-based threats – than on traditional threats, which Article 42(7) TEU, like Article 5 NAT, was originally designed to address. The fact that this strategic focus has remained largely unchanged, even in the face of Russia's war of aggression against Ukraine, suggests that the primacy of NATO's mutual defence obligations over those of the EU is grounded not only in legal hierarchy but also in the EU's limited capacity and mandate in the area of collective defence. While recent EU initiatives reflect growing ambition, they have yet to signal a fundamental rebalancing toward territorial defence.

---

118 Perot, 'The art of commitments' (n 29) 52.
119 Fazio, 'What happens if Trump invades Greenland?' (n 50).
120 Daniel Keohane, 'ESD and NATO' in Giovanni Grevi et al (eds), European Security and Defence Policy: The First 10 Years (1999-2009) (European Union Institute for Security Studies 2009) 131; Reichard (n 24) 130.
121 European Council, Presidency Conclusions, Helsinki, 10-11 December 1999, para 27.
122 Ibid; Blake and Mangiameli (n 16) 1217.
123 Reichard (n 24) 222.
124 Sari (n 21) 406.

2.1 THE 2016 GLOBAL STRATEGY FOR THE EUROPEAN UNION'S FOREIGN AND SECURITY POLICY – SHARED VISION, COMMON ACTION: A STRONGER EUROPE

As the title suggests, the EUGS, which covered not only security and defence but all aspects of EU external action, aimed to initiate a new phase of European integration via common action, rather than merely developing a single strategic vision like the previous 2003 European Security Strategy (ESS).[125]

Unveiled by then-HR/VP Federica Mogherini on 28 June 2016, the EUGS was adopted at a time when Europe was grappling with both internal and external challenges, including Britain's decision to leave the EU, ISIS-driven terrorism,[126] rising migration, and Russia's revanchism, which had culminated in the illegal annexation of the Crimean Peninsula in March 2014, following its recognition of Abkhazia and South Ossetia's independence in August 2008. As a consequence of this new strategic landscape, the word 'defence' was mentioned 57 times in the EUGS – 50 more than in the ESS – with 'strategic autonomy' featuring for the first time in a European strategy document.[127]

'The European Union will promote peace and *guarantee the security of its citizens and territory*', the Strategy claimed,[128] seemingly suggesting that the EU was preparing to take on a more active role in collective defence. To this end, the EUGS called for a sectoral strategy, the Implementation Plan on Security and Defence (IPSD),[129] which aimed to transform the EU into a more autonomous security and defence actor, particularly in the wake of Donald Trump's first election victory as US President on 8 November 2016.[130] This was followed by the adoption of the European Defence Action Plan (EDAP),[131] comprising measures, such as the European Defence Fund (EDF), discussed later in this Section, which were designed

---

[125] Nathalie Tocci, 'The making of the EU Global Strategy' (2016) 37(3) Contemporary Security Policy 461, 462.

[126] Nash Jenkins, 'A Timeline of Recent Terrorist Attacks in Europe' (Time, 20 December 2016) <https://time.com/4607481/europe-terrorism-timeline-berlin-paris-nice-brussels/> accessed 15 August 2025.

[127] The concept had been first mentioned in the European Council Conclusions on CSDP of December 2013 in relation to defence industry, fifteen years after the 1998 Franco-British Saint Malo declaration had called for the Union to develop 'the capacity for autonomous action, backed up by credible military forces […] supported by a strong and competitive European defence industry and technology'. See House of Commons, 'Declaration on European Defence, British-French Summit, St Malo, 3-4 December 1998' (HC 39, 1998-99, UK) <https://publications.parliament.uk/pa/cm199899/cmselect/cmdfence/39/39w17.htm> accessed 13 May 2025.

[128] EUGS (n 4) para 1, 7; emphasis added.

[129] Council of the EU, 'Council conclusions on implementing the EU Global Strategy in the area of Security and Defence' (14149/16, 14 November 2016) <https://www.consilium.europa.eu/media/22459/eugs-conclusions-st14149en16.pdf> accessed 13 May 2025; see also Council of the EU, 'Implementation Plan on Security and Defence' (14392/16, 14 November 2016) <https://www.consilium.europa.eu/media/22460/eugs-implementation-plan-st14392en16.pdf> accessed 18 February 2025.

[130] As pointed out by Sus, 'the unique interinstitutional position of the HR gave Mogherini the advantage in combining the various ideas floating in the policy stream and framing them all as linked to the EUGS's implementation, and thereby achieving wide-ranging policy change'. See, Monika Sus, 'Supranational entrepreneurs: the High Representative and the EU global strategy' (2021) 97(3) International Affairs 823, 840.

[131] European Commission, 'European Defence Action Plan: Towards a European Defence Fund' (Press Release, 30 November 2016) <https://ec.europa.eu/commission/presscorner/detail/en/ip_16_4088> accessed 18 February 2025.

to help EU Member States boost defence research and invest more efficiently on joint defence capabilities.

The 2016 EUGS made express reference to the mutual assistance clause, which had been invoked for the first time only 7 months earlier, in the aftermath of the Paris attacks, for all the reasons and with the implications discussed in detail in the previous sections. 'Mutual assistance' is mentioned no less than 6 times in the document. Among the key priorities of the EU external action, it is stated that

> 'Member States must translate their commitments to mutual assistance and solidarity enshrined in the Treaties into action. The EU will step up its contribution to Europe's collective security, working closely with its partners, beginning with NATO.[132]
> […] While NATO exists to defend its members – most of which are European – from external attack, […] Europeans must be better equipped, trained and organised to contribute decisively to such collective efforts, as well as to act autonomously if and when necessary […]'.[133]

Specifically, the Strategy called for deepening the partnership with NATO 'through coordinated defence capability development, parallel and synchronised exercises, and mutually reinforcing actions to build the capacities of our partners, *counter hybrid and cyber threats*, and promote maritime security'.[134] A month after the Strategy's release, the EU and NATO adopted their first joint declaration, with the purpose of strengthening cooperation in 7 key areas, including hybrid threats, maritime operations, cybersecurity, defence capability development, partner capacity building, defence industry collaboration and joint exercises.[135] On 6 December 2016, the Council[136] and the NAC,[137] endorsed 42 related proposals. The following year, 32 additional proposals were approved expanding cooperation into these as well as new areas such as counterterrorism, women, peace and security, and military

[132] EUGS (n 4) 9.
[133] Ibid 20.
[134] Ibid 37, emphasis added.
[135] European Parliament, 'Joint Declaration by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization' (n 30).
[136] Council of the EU, 'Council Conclusions on the Implementation of the Joint Declaration by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization' (15283/16, 6 December 2016) <https://www.europarl.europa.eu/cmsdata/121581/ST_15283_2016_INIT_EN.pdf> accessed 18 February 2025.
[137] NATO, 'Statement on the implementation of the Joint Declaration signed by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization' (Press Release (2016) 178, 6 December 2016) <https://www.nato.int/cps/en/natohq/official_texts_138829.htm> accessed 18 February 2025.

mobility.[138] In 2018, a second joint declaration[139] introduced another area: resilience to chemical, biological, radiological and nuclear-related (CBRN) risks.

Additionally, the Strategy stated that '[i]ncreased investment in and *solidarity on counter-terrorism* are key' and that 'the EU [would] support the swift recovery of Members States in the event of attacks through enhanced efforts on security of supply, the protection of critical infrastructure, and strengthening the voluntary framework for *cyber crisis management*'.[140]

The 2016 EUGS was followed by three implementation strategies in 2017, 2018 and 2019. The 2017 Implementation Strategy outlined key initiatives intended to advance the EU's role as a security and defence actor. It noted that a Coordinated Annual Review on Defence (CARD) – designed to synchronise Member States' defence planning – had been agreed by the Council, with a first full trial run scheduled for autumn 2017.[141] The Strategy also reported that the Council had resolved to examine the activation of Permanent Structured Cooperation (PESCO), a concept introduced by the 2007 LT,[142] which, according to the Strategy, had 'the potential to make the definitive leap forward in European security and defence'.[143] In addition, it highlighted the establishment of the EDF aimed at incentivising Member States to adopt a more collaborative approach by supporting coordination and enhancement of national defence research spending. Together CARD, PESCO and the EDF were presented as mutually reinforcing instruments, with the European Defence Agency (EDA) identified as playing a key supporting role.[144]

The First Implementation Report also highlighted progress made on EU-NATO cooperation, described as a 'qualitative leap forward'.[145] In addition to the 42 set of proposals agreed in Warsaw, the 2017 Implementation Report referred to the establishment of *a new European Centre for Countering Hybrid Threats in Helsinki* and emphasised joint efforts undertaken by the two organisations in ensuring coherence between the NATO Defence Planning Process (NDPP) and the EU Capability Development Plan (CDP).[146] The 2018 and 2019 Implementation Strategies also highlighted how the EU and NATO had successfully

---

[138] Council of the EU, 'Council conclusions on the Implementation of the Joint Declaration by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization' (14802/17, 5 December 2017) <https://www.consilium.europa.eu/media/31947/st14802en17.pdf> accessed 18 February 2025; NATO, 'Common set of new proposals on the implementation of the Joint Declaration signed by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization' (Press Release (2017) 174, 5 December 2017) <https://www.nato.int/cps/fr/natohq/official_texts_149522.htm?selectedLocale=en> accessed 18 February 2025.

[139] Council of the EU, 'Joint Declaration on EU-NATO Cooperation by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization' (10 July 2018) <https://www.consilium.europa.eu/media/36096/nato_eu_final_eng.pdf> accessed 18 February 2025.

[140] European External Action Service, 'From Shared Vision to Common Action: Implementing the EU Global Strategy: Year 1' (10 January 2017), 21, emphasis added <https://www.eeas.europa.eu/sites/default/files/eugs-report-full_brochure_year_1.pdf> accessed 20 September 2025.

[141] Ibid 22.

[142] TEU (n 2) Article 42(6).

[143] EEAS, 'Implementing the EU Global Strategy: Year 1' (n 140) 22 and 23.

[144] Ibid 23.

[145] Ibid 24.

[146] EEAS, 'Implementing the EU Global Strategy: Year 1' (n 140) 24.

deepened their partnership in the framework of the two joint declarations of 2016 and 2018, especially on military mobility, counterterrorism, cyber and maritime security.[147]

Despite the adoption of new security and defence initiatives, however, none of these documents referred to the mutual defence or the solidarity clauses. The Council Conclusions of June 2019 called on 'Member States to discuss the lessons identified following the first activation of Article 42.7 TEU'[148] and reminded them of the importance of mutual assistance and solidarity. Yet, there is no indication that such discussions have taken place.

2.2 THE 2022 STRATEGIC COMPASS FOR SECURITY AND DEFENCE

The product of a two-year reflection process conducted by former HR/VP Joseph Borrell in tandem with the European Commission and EU Member States,[149] the Strategic Compass was adopted by the Foreign Affairs and Defence Ministers of the 27 EU Member States on 21 March 2022, roughly a month after the war in Ukraine started, and endorsed by EU Heads of State and Government a few days later. Unlike previous EU security strategies, the Strategic Compass is characterised by a common threat analysis and a bottom-up approach.[150]

The word 'defence' is mentioned no fewer than 234 times in the strategy – including, for the first time ever, in the title – over 4 times more than in the EUGS, reflecting the heightened emphasis on defence as a consequence of war on the EU's doorstep. In addition, mutual assistance is referred to 12 times in the Compass – twice as much than in the previous strategy.

In order to be able to act more rapidly and assertively, EU Member States have agreed in the Compass to develop an RDC of up to 5,000 troops by 2025. The RDC will replace the EU Battlegroups, multinational rapid reaction forces created for crisis management operations outside the EU which had become operational in 2007 but were never deployed. For the first time, the EU also stated its intention to conduct regular live exercises to increase defence interoperability and readiness. 'We will continue to invest in our mutual assistance under Article 42(7) of the Treaty on European Union as well as solidarity under Article 222 of the Treaty on the Functioning of the European Union, in particular through frequent exercises', the Compass states.[151] However, as with the previous strategy, the focus seems to remain on non-traditional threats. As Fiott has pointed out,[152] these regular exercises seem, in fact, to be mostly aimed at responding to non-traditional attacks such as cyber attacks,[153]

---

[147] European External Action Service, 'Implementing the EU Global Strategy: Year 2' (25 June 2018), 8 <https://www.eeas.europa.eu/sites/default/files/eugs_annual_report_year_2.pdf> accessed 24 February 2025; European External Action Service, 'The European Union's Global Strategy Three Years On, Looking Forward' (13 June 2019), 11 <https://www.eeas.europa.eu/sites/default/files/eu_global_strategy_2019.pdf> accessed 24 February 2025.

[148] Council of the EU, 'Council Conclusions on Security and Defence in the context of the EU Global Strategy' (10048/19, 17 June 2019) <https://www.consilium.europa.eu/media/39786/st10048-en19.pdf> accessed 24 February 2025.

[149] Council of the EU, 'Council Conclusions on Security and Defense' (8910/20, 17 June 2020) <https://www.consilium.europa.eu/media/44521/st08910-en20.pdf> accessed 24 February 2025. See also, Monika Sus, 'Exploring the dynamics of policy change in EU security and defence: policy entrepreneurs behind the Strategic Compass' (2023) 47(4) West European Politics 942, 948, 951, 952, 953, 954 and 956.

[150] EEAS, 'A Strategic Compass for Security and Defence' (n 4) 7.

[151] Ibid 28. France played a leading role in pushing for this. See, e.g., Sus, 'Exploring the dynamics of policy change in EU security and defence' (n 149) 954.

[152] Fiott, 'Rising Risks' (n 113).

[153] EEAS, 'A Strategic Compass for Security and Defence' (n 4) 35 and 39.

hybrid attacks[154] and even space-based attacks.[155] Indeed, as Blockmans et al also noted, there is a strong focus on hybrid threats and tactics (the term hybrid appears 46 times) in the Compass, which 'seems out of sync with the fact that Russia is waging a highly conventional war against Ukraine […]'.[156] A strong emphasis is placed on the development of *the EU Hybrid Toolbox*, *the Cyber Resilience Act*, and further development of *the Cyber Diplomacy Toolbox*, the Foreign Information Manipulation and Interference (FIMI) Toolbox and adoption of *the EU Space Strategy for security and defence*.

There is no mention in the Compass of how the EU intends to prepare for the eventuality of a traditional attack on its soil amid Russia's aggression of Ukraine. The Compass merely states that the EUMS could play a role in 'the coordination of logistical support and assistance to Member States and third countries in a crisis, as well as the implementation of EU instruments such as the European Peace Facility or, upon Member States' request, the mutual assistance clause, in line with the Treaty on European Union'.[157] This is because most EU Member States are also members of NATO and consider its mutual defence guarantee, enshrined in Article 5 NAT, the cornerstone of their security. However, following the outcome of the 2024 US Presidential election, which saw Donald Trump elected for a second non-consecutive term, this reliance faces new strategic uncertainty.[158] With the potential to unlock €800 billion for defence, the ReArm Europe Plan/Readiness 2030 – unveiled by the European Commission two months after Trump's return to the White House – is a clear attempt to develop autonomous defence capabilities and reduce dependency from the US. The recent agreement between France and the UK to deepen bilateral cooperation on nuclear deterrence[159] can also be seen as a direct response to the growing uncertainty surrounding the US nuclear umbrella, despite reassurances made at the NATO Hague Summit.[160]

As in the previous Strategy, considerable attention is given to the EU-NATO relationship. The Executive Summary states that 'A stronger and more capable EU in the field of security and defence will contribute positively to global and transatlantic security and is complementary to *NATO, which remains the foundation of collective defence for its members*'. The partnership with NATO is the first topic addressed in the 'Partner' section – one of four pillars of the Compass, alongside Act, Secure, and Invest. 'The EU's strategic partnership with NATO is essential for our Euro-Atlantic security', the Compass affirms.[161] The

---

[154] Ibid 34 and 39.
[155] Ibid 34 and 36.
[156] Steven Blockmans et al, 'The EU's Strategic Compass – A guide to reverse strategic shrinkage?' (CEPS Policy Insights 2022, Centre for European Policy Analysis, 14 March 2022), 8 <https://cdn.ceps.eu/wp-content/uploads/2022/03/CEPS-PI2022-14_EU-Strategic-Compass.pdf> accessed 24 February 2024.
[157] EEAS, 'A Strategic Compass for Security and Defence' (n 4) 38.
[158] Fazio, 'Collective defence in NATO' (n 18) 8-9. See also Emma Ashford and MacKenna Rawlins 'American Roulette: Scenarios for US Retrenchment and the Future of European Defense' (Policy Paper, Stimson Center, 8 July 2024) <https://www.stimson.org/2024/american-roulette-scenarios-for-us-retrenchment-and-the-future-of-european-defense/> accessed 20 September 2024.
[159] UK Prime Minister's Office and The Rt Hon Sir Keir Starmer KCB KC MP, 'Northwood Declaration: 10 July 2025 (UK-France joint nuclear statement)' (Press Release, 10 July 2025) <https://www.gov.uk/government/news/northwood-declaration-10-july-2025-uk-france-joint-nuclear-statement> accessed 12 July 2025.
[160] Federica Fazio, 'A Dissenting Opinion on The Hague Summit: the Real Winner is NATO, Not Trump' (DCU Brexit Institute, 30 June 2025) <https://www.dcu.ie/blog/2151/dissenting-opinion-hague-summit-real-winner-nato-not-trump> accessed 8 July 2025.
[161] EEAS, 'A Strategic Compass for Security and Defence' (n 4) 53, emphasis added.

document claims that cooperation with NATO will be further strengthened in the areas covered by the 2016 and 2018 Joint Declarations.[162]

The real game changer, according to the Compass, however, will be 'moving to joint and inclusive exercises', which will allow the two organisations to build trust, increase interoperability and deepen cooperation.[163] In 2022, under the Plan for Implementation of Parallel and Coordinated Exercises (PACE) 2022-2023, NATO staff joined the planning and conduct phases of the EU Integrated Resolve (IR) 22 exercise, focusing on the *management of hybrid crises* with internal and external dimensions.[164] The following March, staff from the European Commission, the General Secretariat of the European Council, the Council, and the EEAS participated in the planning and conduct of NATO's crisis management exercise (CMX) 2023, *also focusing on a hybrid crisis scenario*.[165]

Finally, the Strategic Compass stresses the need to invest more and better in defence capabilities and cutting-edge technologies.

The Strategic Compass was followed by two Progress Reports in 2023 and 2024.

In relation to the mutual defence clause specifically, the 2023 Progress Report stated that '[t]o further strengthen our mutual assistance in case of an armed aggression, we have conducted exercises on Article 42(7) TEU in scenarios involving *cyber, hybrid and space-related threats*, and will continue to do so on a regular basis'.[166] This claim was reiterated in the 2024 Progress Report, which stressed that the EU 'will continue to organise and conduct regular exercises with regard to Article 42(7)'.[167] In fact, the bulk of the 'Secure' sections in both Reports focuses on *countering hybrid, cyber and space threats*. This appears to confirm the earlier point: despite a shared recognition of the threat posed by the Russian Federation, the EU has yet to implement a credible military deterrent against it, despite calls from the European Parliament to operationalise Article 42.7 TEU[168] and clarifying its relationship with Article 5 NAT.[169]

The 2023 Progress Report also highlighted the role played by the EPF, which replaced and expanded the scope of the Athena mechanism and the African Peace Facility (APF) in 2018.[170] The report described the EPF as 'a game changer', as it has enabled the EU to

---

[162] Ibid.
[163] Ibid 54.
[164] For more information, see <https://www.eeas.europa.eu/eeas/eu-integrated-resolve-2022-eu-ir22-parallel-and-coordinated-exercisespace_en> accessed 26 April 2024.
[165] For more information, see <https://www.nato.int/cps/en/natohq/news_212527.htm> accessed 26 April 2024.
[166] European External Action Service, 'Annual Progress Report on the Implementation of the Strategic Compass for Security and Defence' (20 March 2023) 9, emphasis added <https://www.eeas.europa.eu/sites/default/files/documents/2023/StrategicCompass_1stYear_Report.pdf> accessed 26 April 2025.
[167] European External Action Service, 'Annual Progress Report on the Implementation of the Strategic Compass for Security and Defence' (18 March 2024), 12, emphasis added <https://www.eeas.europa.eu/eeas/2024-progress-report-implementation-strategic-compass-security-and-defence_en> accessed 26 April 2024..
[168] European Parliament, 'Implementation of the common security and defence policy – annual report 2022 (2022/2050(INI))' P9_TA(2023)0010, para 3.
[169] European Parliament, 'Implementation of the common security and defence policy – annual report 2024 (2024/2082(INI))' P10_TA(2025)0058, para 9.
[170] Article 41(2) TEU prohibits the financing of EU military operations through the EU budget, but Article 41(3) allows the Council to establish special mechanisms to manage the financing of the common costs of military operations. The Athena mechanism, established by Council Decision 2004/197/CFSP [2004] OJ

provide Ukraine with both non-lethal and lethal assistance[171] – something Rasi has described as the EU's 'first exercise of collective self-defence'.[172] The 2024 Progress report further noted the importance of the establishing of a dedicated Ukraine Assistance Fund (UAF) within the EPF.

With regards to the RDC, the Progress Reports claim that work to adapt the Battlegroups and operationalise the RDC is ongoing; three operational scenarios have been finalised on rescue and evacuation, the initial phase of stabilisation, and military support to humanitarian assistance and disaster relief.[173] Although designed for crisis management operations outside the EU, like its NATO counterpart, the NATO Response Force (NRF), replaced by the Allied Response Force (ARF) in July 2024, the RDC could also be employed for territorial defence. However, it is important to note that, at its launch, the NRF was nearly twice as large, with 9,500 troops;[174] the brigade-size force envisioned by the RDC may prove insufficient to respond to a crisis, let alone an armed aggression, and represents a further decrease in the EU's level of ambition compared to the 6,000 troops envisaged by the Battlegroups.[175] Therefore, much like its predecessors, the RDC might 'remain a paper tiger and lack concrete use'.[176]

Finally, the two reports highlighted progress made in strengthening the partnership with NATO. A Task Force on the resilience of critical infrastructures was established in June 2023 within the framework of the EU-NATO Structured Dialogue on Resilience in response to the sabotage of the Nord Stream pipelines, and a first structured dialogue on Space took place in December 2023.[177] Additionally, in January 2023, the two organisations had also agreed on a third joint declaration. The declaration notes progress made in the areas of the 2016 and 2018 declarations, condemns Russia's unlawful invasion of Ukraine, and announces that the EU and NATO will take their partnership 'to the next level'.[178] However, there is still no mention in the declaration of how the EU and NATO's mutual defence clauses relate to each other.

The 2023 Progress Report used identical language, adding that the EU's 2022 Strategic Compass and NATO's 2022 Strategic Concept 'provide a solid basis to further expand the

---

L63/68, and the APF, created through Council Decision No 3/2003 of the ACP-EC Council of Ministers of 11 December 2003 [2003] OJ L345/108, were two such mechanisms.

171 2023 Progress Report, (n 166), at 8.

172 Aurora Rasi, 'Providing Weapons to Ukraine: The First Exercise of Collective Self-defence by the European Union?', 9/1 European Papers (2024), 397-422.

173 2023 Progress Report (n 166) 8 and 9; 2024 Progress Report (n 167) 12.

174 Guillaume Lasconjarias, 'The NRF: from a Key Driver of Transformation to a Laboratory of the Connected Forces Initiatives' (Research paper, NATO Defence College 88, January 2023), 4 <https://www.files.ethz.ch/isn/157613/rp_88.pdf> accessed 20 September 2024.

175 The 1999 Helsinki Headline Goal aimed to develop a European Rapid Reaction Force by 2003 consisting of up to 15 brigades totalling up to 60,000 troops, ready to deploy within 60 days and sustain operations for at least one year. The 2010 Headline Goal scaled down the force from 15 brigades to 4 battalion-sized rapid response units (EU Battlegroups) totalling 6,000 troops, designed to deploy within 10 days of an EU decision, and sustain operations for 30 days, extendable to 120 days if resupplied.

176 Blockmans et al (n 156) 3.

177 2024 Progress Report (n 167) 24; 2023 Progress Report (n 166) 19.

178 NATO, 'Joint Declaration on EU-NATO Cooperation by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization' (10 January 2023) <https://www.nato.int/cps/en/natohq/official_texts_210549.htm> accessed 6 September 2024

partnership'.[179] Progress made in the implementation of the current 74 proposals has been reviewed 10 times (in June[180] and November 2017,[181] in June 2018,[182] 2019,[183] 2020,[184] 2021,[185] 2022,[186] 2023,[187] 2024[188] and 2025)[189] so far. The latest progress report, issued in June 2025, stresses the importance of developing an even more robust, coherent and complementary EU-NATO partnership.[190]

It is important to note that beyond PACE, the European Commission also participated in NATO's exercises such as STEADFAST DUEL 2024 and – together with the EUMS – STEADFAST DETERRENCE and STEADFAST DAGGER 2024.[191] However, the EU did not participate in STEADFAST DEFENDER 2024, NATO's largest Article 5 exercise since the Cold War, which was aimed at testing the Alliance's new defence plans and its ability to rapidly deploy forces in defence of continental Europe. This reflects the fact that the EU's focus – and that of its cooperation with NATO – remains primarily

---

[179] 2023 Progress Report (n 166) 18 and 19.
[180] NATO, 'Progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016' (14 June 2017) <https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_06/20170619_170614-Joint-progress-report-EU-NATO-EN.pdf> accessed 23 May 2025.
[181] NATO, 'Second progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016' (29 November 2017) <https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_11/171129-2nd-Joint-progress-report-EU-NATO-eng.pdf> accessed 23 May 2025.
[182] NATO, 'Third progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016 and 5 December 2017' (8 June 2018) <https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_06/20180608_180608-3rd-Joint-progress-report-EU-NATO-eng.pdf> accessed 23 May 2025.
[183] NATO, 'Fourth progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016 and 5 December 2017' (17 June 2019) <https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_06/190617-4th-Joint-progress-report-EU-NATO-eng.pdf> accessed 23 May 2025.
[184] NATO, 'Fifth progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016 and 5 December 2017' (16 June 2020) <https://www.nato.int/nato_static_fl2014/assets/pdf/2020/6/pdf/200615-progress-report-nr5-EU-NATO-eng.pdf> accessed 23 May 2025.
[185] NATO, 'Sixth progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016 and 5 December 2017' (3 June 2021) <https://www.nato.int/nato_static_fl2014/assets/pdf/2021/6/pdf/210603-progress-report-nr6-EU-NATO-eng.pdf> accessed 20 September 2025.
[186] NATO, 'Seventh progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016 and 5 December 2017' (20 June 2022) <https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/220620-progress-report-nr7-EU-NATO-eng.pdf> accessed 23 May 2025.
[187] NATO, 'Eight progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016 and 5 December 2017' (16 June 2023) <https://www.nato.int/nato_static_fl2014/assets/pdf/2023/6/pdf/230616-progress-report-nr8-EU-NATO.pdf> accessed 23 May 2025.
[188] NATO, 'Ninth progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016 and 5 December 2017' (13 June 2024) <https://www.nato.int/nato_static_fl2014/assets/pdf/2024/6/pdf/240613-progress-report-nr9-EU-NATO.pdf> accessed 23 May 2025.
[189] NATO, 'Tenth progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017' (10 June 2025) <https://www.nato.int/nato_static_fl2014/assets/pdf/2025/6/pdf/250605-progress-report-nr10-EU-NATO.pdf> accessed 12 June 2025.
[190] Ibid 1.
[191] Ibid 11.

geared toward crisis management, prevention, and defence against non-traditional threats, rather than conventional territorial defence.

3 CONCLUSION

This article has examined the EU's mutual assistance clause to understand how credible it is and the type of legal responsibilities it imposes on the members of the Union. Today, the mutual defence clause, enshrined in Article 42(7) TEU and introduced almost two decades ago in Lisbon, provides a legal framework for EU Member States to engage in collective defence similar to Article 5 NAT for NATO Allies. It does so by committing them to an *obligation of result rather than means*.

The legal analysis has shown that the more ambiguous phrasing '*by all the means in their power*' employed by Article 42(7) TEU permits both civil and military assistance to be provided to EU members under aggression, while prioritising the achievement of the intended result. This means that, much like NATO Allies, EU Member States are left free to choose the means of assistance in a case of aggression. Therefore, although the obligations imposed by Article 42(7) TEU might seem more stringent than those imposed by Article 5 NAT, these obligations are, nonetheless, *obligations of result and not means*. Yet, unlike NATO's, these obligations are *automatic*, as they require no formal Council decision or conclusion to be implemented. At the same time, however, the presence of the Irish and NATO clauses renders these obligations *conditional*, as the means of assistance to be provided must align with the foreign and security policies of both neutral and non-aligned countries, in addition to those of NATO countries, collectively encompassing the totality of EU Member States.

Section 1.6 has explained that neutral and non-aligned members, as well as those requiring parliamentary authorisation of the use of force, are not exempted from providing assistance under Article 42(7) TEU. For the remaining 23 EU Member States, which are also NATO Allies, mutual defence obligations under Article 42(7) TEU apply, provided they do not conflict with those under Article 5 NAT. Importantly, however, the legal primacy of Article 5 does not grant NATO a 'right of first refusal', as illustrated by France's invocation of the EU's mutual defence clause in 2015 despite its NATO membership. Moreover, triggering the EU's Article 42(7) does not automatically activate NATO's Article 5, although the simultaneous invocation of both clauses by shared members is not precluded.

Finally, the section has pointed out that Article 42(7) TEU could potentially be triggered by a non-NATO EU Member State against a non-EU NATO Ally. Additionally, in the event of an attack, EU neutral or non-aligned countries could indirectly benefit from NATO's mutual security guarantee through their partnerships with NATO Allies. Similar to NATO though, no sanctioning mechanism exists to compel EU Member States to act in case of inaction or inadequate action, as the CFSP and CSDP fall outside the jurisdiction of the CJEU.

The strategic analysis has focused on the growing importance the EU has been placing on defence, and particularly the mutual defence clause, and related initiatives in this respect, including in cooperation with NATO. Although NATO remains the cornerstone of European defence, there are clear indications that, since 2016 (and even more so since 2022), the EU has been actively seeking to retool its CSDP instruments in response to the changing and more complex threat environment in order to play a more active role in defence.

The 2022 Strategic Compass has undoubtedly marked an important shift in the EU's approach to security and defence by providing a common threat analysis. However, much like the 2016 EUGS, despite the increased emphasis on the mutual defence clause and a stronger EU-NATO partnership, there seems to be a disproportionate focus by the EU on unconventional threats, such as potential cyber, hybrid and space attacks, without addressing how to prepare for traditional, large-scale military attacks. This has to do with the fact that the EU as a whole has no collective defence mandate, as Article 42(7) TEU envisions no formal role for the EU in the event of armed aggression on EU territory. While, in principle, both Article 5 NAT and Article 42(7) TEU cover traditional and non-traditional attacks, territorial defence continues to be viewed as the responsibility of NATO.

The start of the second Trump Presidency, with its uncertain commitment to defend not just Ukraine but NATO Allies as well, has intensified debates on European strategic autonomy and ways to reduce reliance on the US. The ReArm Europe Plan/Readiness 2030 and its Security Action for Europe (SAFE) fund,[192] represent a clear move in this direction, as do the White Paper for European Defence – Readiness 2030[193] and the recently proposed 2028-2034 Multiannual Financial Framework – worth nearly €2 trillion, the largest in the EU's history – of which €131 billion is earmarked for security, defence and space through the European Competitiveness Fund.[194]

However, building a competitive and autonomous European defence industry will not happen overnight. The EU remains highly dependent on American technology, including the F-35 fighter jets produced by Lockheed Martin – of which it has no equivalent alternative – as well as Patriot missile defence systems and other critical enablers. This dependence was further cemented in the recent EU-US Framework Agreement, under which the EU agreed 'to substantially increase procurement of military and defence equipment from the United States.'[195]

Therefore, despite the EU's response to the war in Ukraine and its post-2022 initiatives, the EU's ability to credibly threaten the use of force in the exercise of the right of collective defence remains a distant prospect, contingent, on the one hand, on the development of a common defence under Article 42(2) TEU or, potentially, through an intergovernmental arrangement outside of the EU legal framework, and, on the other, on the development of a strong European defence industrial base.

---

[192] As the first pillar of the ReArm Europe Plan/Readiness 2030, this instrument aims to mobilise up to €150 billion in investments, reinforcing the EU's ability to act collectively in the security and defence domain. At the time of writing, 19 EU Member States have already expressed an interest and more are expected to do so ahead of the formal deadline for application of 30 November 2025. See European Commission, Defence Industry and Space 'SAFE | Security Action for Europe', (30 July 2025), available <https://defence-industry-space.ec.europa.eu/eu-defence-industry/safe-security-action-europe_en> accessed 18 August 2025.

[193] European Commission, 'White Paper for European Defence – Readiness 2030' (12 March 2025) <https://commission.europa.eu/document/download/e6d5db69-e0ab-4bec-9dc0-3867b4373019_en> accessed 8 April 2025.

[194] European Commission, 'The 2028-2034 EU budget for a stronger Europe' (16 July 2025) <https://commission.europa.eu/strategy-and-policy/eu-budget/long-term-eu-budget/eu-budget-2028-2034_en> accessed 18 August 2025.

[195] Framework Agreement, (n 5) para 7.

LIST OF REFERENCES

Blake HJ and Mangiameli S, 'Article 42 [CSDP: Goals and Objectives; Mutual Defence] (ex-Article 17 TEU)' in Blake HJ and Mangiameli S (eds), The Treaty on European Union (TEU): A Commentary (Berlin: Springer-Verlag Berlin Heidelberg 2013)
DOI: https://doi.org/10.1007/978-3-642-31706-4_43

Cane P, 'Context, context everywhere' (2020) 16(4) International Journal of Law in Context 459
DOI: https://doi.org/10.1017/S1744552320000208

Donaldson M, 'Peace, war, law: teaching international law in contexts' (2022) 18(4) International Journal of Law in Context 393
DOI: https://doi.org/10.1017/S1744552322000350

Dyson T and Konstadinides T, 'The Legal Underpinnings of European Defence Cooperation' in Dyson T and Konstadinides T (eds), European Defence Cooperation in EU Law and IR Theory (Palgrave Macmillan 2013)
DOI: https://doi.org/10.1057/9781137281302_3

Fabbrini F, 'Funding the War in Ukraine, the European Peace Facility, the Macro-Financial Assistance Instrument, and the Slow Rise of and EU Fiscal Capacity' (2023) 11(4) Politics & Governance 52
DOI: https://doi.org/10.17645/pag.v11i4.7174

— —, 'To "Provide for the Common Defence": Developments in Foreign Affairs and Defence' in Fabbrini F (ed), The EU Constitution in Time of War (Oxford University Press 2025)
DOI: https://doi.org/10.1093/oso/9780198963486.001.0001

Fazio F, 'Collective defence in NATO: A legal and strategic analysis of Article 5 in light of the war in Ukraine' (DELI Working Paper Series 2/24, Dublin European Law Institute, 5 November 2024) <https://zenodo.org/records/14037328> accessed 20 September 2025

Fiott D, 'In every crisis an opportunity? European Union integration in defence and the War on Ukraine' (2023) 45(3) Journal of European Integration 447
DOI: https://doi.org/10.1080/07036337.2023.2183395

Geursen WW, Mapping the territorial scope of EU law (PhD thesis, Vrije Universiteit Amsterdam 2024)
<https://research.vu.nl/ws/portalfiles/portal/307385687/ww%20geursenmapping%20the%20territorial%20scope%20of%20eu%20lawthesis%20including%20annexes%20-%2065e4818190907.pdf> accessed 20 September 2025

Howorth J, 'The European Draft Constitutional Treaty and the Future of the European Defence Initiative: A Question of Flexibility' (2004) 9(4) European Affairs Review 483
DOI: https://doi.org/10.54648/EERR2004039

Koutrakos P, 'Judicial Review in the EU's Common Foreign and Security Policy' (2018) 67(1) International and Comparative Law Quarterly 1
DOI: https://doi.org/10.1017/S0020589317000380

Martin JC, 'La Clause de Défense Mutuelle' in Bernard E, Loïez Q and Stéphane Rodrigues (eds), L'Union européenne de la défense: commentaire article par article (Bruylant 2024)

Orakhelashvili A, '1969 Vienna Convention. Article 30: Application of Successive Treaties Relating to the Same Subject Matter' in Corten O and Klein P (eds), The Vienna Convention on the Law of Treaties A Commentary (Oxford University Press 2011)
DOI: https://doi.org/10.1093/law/9780199573530.003.0121

Perot E, 'The art of commitments: NATO, the EU, and the interplay between law and politics within Europe's collective defence architecture' (2019) 28(1) European Security 40
DOI: https://doi.org/10.1080/09662839.2019.1587746

— —, 'The European Union's nascent role in the field of collective defense: between deliberate and emergent strategy' (2024) 46(1) Journal of European Integration 1
DOI: https://doi.org/10.1080/07036337.2023.2237653

Rasi A, 'Providing Weapons to Ukraine: The First Exercise of Collective Self-defence by the European Union?' (2024) 9(1) European Papers 397
DOI: https://doi.org/10.15166/2499-8249/763

Reichard M, 'Collective Self-Defence' in Reichard M (ed), The EU-NATO Relationship: A Legal and Political Perspective (Routledge 2006)
DOI: https://doi.org/10.4324/9781315616322

Sari A, 'The Mutual Assistance Clauses of the North Atlantic and EU Treaties: The Challenge of Hybrid Threats' (2019) 10 Harvard National Security Journal 405

Smith SJ and Gebhard C, 'EU–NATO relations: running on the fumes of informed deconfliction' (2017) 26(3) European Security 303
DOI: https://doi.org/10.1080/09662839.2017.1352581

Sus M, 'Supranational entrepreneurs: the High Representative and the EU global strategy' (2021) 97(3) International Affairs 823
DOI: https://doi.org/10.1093/ia/iiab037

— —, 'Exploring the dynamics of policy change in EU security and defence: policy entrepreneurs behind the Strategic Compass' (2023) 47(4) West European Politics 1
DOI: https://doi.org/10.1080/01402382.2023.2232704

Tocci N, 'The making of the EU Global Strategy' (2016) 37(3) Contemporary Security Policy 461
DOI: https://doi.org/10.1080/13523260.2016.1232559

Twinning W, Law in Context: Enlarging a Discipline (Oxford University Press 1997)

THE MISSING CLIMATE DIMENSION IN THE EU AI ACT: PARSING THE WORLD'S FIRST COMPREHENSIVE AI REGULATION THROUGH THE LENS OF THE EUROPEAN GREEN DEAL

STANISLOVAS STAIGVILAS*

The European Union's Artificial Intelligence Act (AI Act) marks the first attempt by a major global jurisdiction to establish a harmonised legal framework for artificial intelligence. While commendable in its emphasis on fundamental rights and technological safety, the AI Act is strikingly silent on the climate action. The article interrogates this lacuna in the light of the European Green Deal and the objective of the Union policy to combat climate change enshrined in Article 191(1) TFEU. Through doctrinal analysis of the AI Act's risk-based structure, conformity assessment regime and delegated governance procedures, the article argues that the absence of climate safeguards represents a failure of policy coherence. It critiques the AI Act's inability to classify climate-relevant AI systems as high-risk, its neglect of energy and emissions transparency and its omission of climate due diligence in regulatory sandboxes. Drawing on both legal doctrine and comparative insights, the article proposes regulatory reforms to embed climate-conscious obligations into AI governance, thus realigning the AI Act with the Union's binding climate commitments and broader constitutional identity as a normative green power.

1 INTRODUCTION

The European Union (EU) has historically positioned itself at the vanguard of global regulation in response to disruptive technological developments. Its responses to past waves of technological change – such as the controversies over genetically modified organisms (GMOs) in the 1990s, the adoption of the General Data Protection Regulation (GDPR) in 2016 and the recent Digital Services Act (DSA) and Digital Markets Act (DMA) – demonstrate a consistent regulatory logic: cautious, rights-based and focused on safeguarding public goods in the face of rapid innovation.

Continuing this tradition, the Artificial Intelligence Act – adopted as Regulation (EU) 2024/1689 – represents the world's first comprehensive legislative framework on artificial intelligence, setting a benchmark for global AI governance.[1] It is a horizontally applicable, cross-sectoral regulation that classifies AI systems into four risk tiers (minimal, limited, high, and

* Mr. Stanislovas Staigvilas is a legal researcher based in Brussels, specializing in EU law and policy. He holds an LLM cum laude in European Private Law.

[1] Regulation (EU) 2024/1689 of the European Parliament and of the Council 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) [2024] OJ L2024/1689.

unacceptable) and establishes corresponding obligations across their development, deployment, and post-market stages. It also introduces new governance structures, including the European Artificial Intelligence Office, and lays out detailed requirements for conformity assessments, CE marking and fundamental rights impact evaluations.

Although widely praised for embedding Union values – notably human dignity, privacy and safety – into digital regulation, the AI Act exhibits a profound and consequential omission: it fails to address the climate-related impacts of artificial intelligence. This is particularly alarming in light of the Union's legally binding climate objectives under the European Green Deal,[2] the European Climate Law,[3] and, additionally, the overarching duty to ensure environmental integration across all policy domains as enshrined in Article 11 of the Treaty on the Functioning of the European Union (TFEU).[4] Notably, the AI Act does not:

- classify energy-intensive, emissions-heavy AI systems as inherently 'high-risk' (Annex III);
- incorporate climate-related performance criteria into the conformity assessment procedures, as governed by Article 43 § 5 of the EU AI Act;
- impose any duty of climate due diligence or energy transparency on AI providers or deployers; or
- integrate climate safeguards in regulatory sandboxes or post-market oversight mechanisms.

This regulatory blind spot carries important legal and systemic consequences. As recent scholarship has sharply observed,[5] the EU AI Act reveals a deeper structural misalignment between the Union's climate strategy and its digital transformation agenda – two pillars of the twin transition. The Act's risk-based classification model, though robust in its attention to fundamental rights, safety, and transparency, remains climate-wise agnostic. It does not account for the substantial energy consumption, lifecycle emissions or carbon intensity of AI systems and infrastructures. This omission undermines the internal consistency of the EU's broader legal architecture by perpetuating a siloed approach to governance – where climate law and digital regulation evolve in parallel but uncoordinated regimes. As a result, the AI Act not only fails to reflect the EU's climate neutrality objective under the Green Deal but also risks weakening regulatory coherence across key sectors such as data, energy, trade, and industrial policy.

Similarly, civil society organisations have also raised concerns about the omissions in respect of climate mitigation in the EU AI Act. AlgorithmWatch, a non-governmental and

---

[2] European Commission, 'Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: The European Green Deal' COM(2019) 640 final.

[3] Regulation (EU) 2021/1119 of the European Parliament and of the Council of 30 June 2021 establishing the framework for achieving climate neutrality and amending Regulations (EC) No 401/2009 and (EU) 2018/1999 ('European Climate Law') [2021] OJ L243/1.

[4] Consolidated Version of the Treaty on the Functioning of the European Union [2012] OJ C326/47, Article 11.

[5] Paulo Carvão et al, 'Governance at a Crossroads: EU AI Regulation and Environmental Policy' (M-RCBG Associate Working Paper Series No. 251, Harvard Kennedy School, 2024) <https://www.hks.harvard.edu/sites/default/files/Final_AWP_251_2.pdf> accessed 1 September 2025.

non-profit organisation based in Germany which advocates for algorithmic systems that advance justice, democracy, human rights and sustainability, has been particularly outspoken. During the trilogue negotiations, it sharply criticised the AI Act, arguing that it overlooks a critical opportunity to ensure that the development and use of AI systems align with the imperatives of climate sustainability. By neglecting the carbon intensity and resource demands of AI, the Act risks undermining the Union's collective effort to combat climate change and runs counter to the objectives of the European Green Deal and related policy frameworks. Since negotiations are still ongoing, there remains an important window to remedy this omission. A necessary first step would be to recognise the climate risks of AI explicitly, making them a relevant criterion in determining whether systems fall within the high-risk category. Building on this, developers and deployers of AI should be required to monitor the greenhouse gas emissions and energy use associated with their systems, disclose this data transparently and take concrete measures to minimise their climate footprint throughout the lifecycle of AI technologies. It also warned that the current framework risks 'entrenching AI infrastructure that is incompatible with the EU's climate goals'.[6]

This article contends that the AI Act, in its current form, suffers from a systemic deficiency: it fails to meaningfully integrate climate mitigation into the legal governance of Europe's digital transformation. This is not a mere legislative oversight, but a deeper signal of dissonance between the Union's digital ambitions and its Treaty-enshrined climate commitments. The omission fractures the coherence of EU law at a time when its regulatory architecture is being watched – and emulated – globally. As the world's first attempt to comprehensively govern artificial intelligence, the EU AI Act is more than a legal milestone: it is a constitutional moment – a test of the Union's ability to reconcile innovation with planetary responsibility. If that test is to be passed, the Act must evolve beyond its compartmentalised design. What is needed now is a new regulatory paradigm – one that does not treat sustainability as a policy accessory, but as a foundational design principle. Under the shadow of a global climate reckoning, technological ambition must no longer compete with ecological stewardship. It must be its ally.

2 MAPPING THE EUROPEAN UNION'S LEGISLATIVE ARCHITECTURE: DIGITAL AND CLIMATE DIMENSIONS IN PARALLEL

In the labyrinthine architecture of European Union law, where directives, regulations, delegated acts, and policy communications proliferate with remarkable velocity, it is vital to pause and apprehend the panoramic structure of the legislative terrain.

[6] Nikolett Aszódi, 'AI Act Trilogue Ignores Environmental Impact of Artificial Intelligence' (*AlgorithmWatch*, 5 December 2023) <https://sustain.algorithmwatch.org/en/the-eus-ai-act-dangerously-neglecting-environmental-risks/> accessed 1 September 2025.

2.1 THE EU'S DIGITAL LEGISLATIVE FRAMEWORK: A HORIZONTAL OVERVIEW

Over the past decade, the European Union has enacted a sweeping array of legislative instruments aimed at governing the digital domain. This surge of lawmaking – often described as a case of regulatory or legislative inflation – has produced a multi-layered and densely populated legal ecosystem. The European Strategy for Data,[7] the Digital Decade 2030 policy programme[8] and other flagship pieces of EU digital legislation have together framed digital transformation as a strategic imperative – one that has since been pursued through a rapid and expansive legislative agenda. What has emerged is a horizontal digital rulebook: a framework of interlocking regulations that together shape platform governance, data access, competition, AI deployment and market design.

2.1[a] General Data Protection Regulation (GDPR)

The General Data Protection Regulation,[9] adopted on 27 April 2016, remains the European Union's foundational legal instrument governing the processing of personal data. As a directly applicable regulation, it harmonises data protection rules across all Member States and reinforces the individual's right to informational self-determination. The GDPR introduced key principles such as lawfulness, fairness and transparency, data minimisation, purpose limitation, and accountability, and it established powerful enforcement tools, including administrative fines of up to 4% of global annual turnover. In addition to its normative weight, the GDPR has exercised significant extraterritorial influence, becoming a global reference point for data protection law. Yet, despite its emphasis on safeguarding fundamental rights in the digital sphere, the Regulation is structurally silent on climate-compatible sustainability. It contains no provisions that address the energy costs of data storage and transfer or the resource intensity of large-scale data processing systems. As such, the GDPR exemplifies a model of digital fundamental rights regulation in which climate considerations are not yet part of the legal calculus – a legacy that persists across the EU's digital legislative landscape.

At the time of writing, the European Commission has proposed targeted reforms to the GDPR as part of the SME Relief Package, following Mario Draghi's recommendations on regulatory agility. The draft introduces new business categories under Article 4, including 'small mid-cap enterprises' (SMCs), defined as organisations with fewer than 750 employees and subject to forthcoming financial thresholds. Article 30(5) raises the record-keeping exemption

[7] European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European Strategy for Data' COM(2020) 66 final.
[8] European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: 2030 Digital Compass – The European Way for the Digital Decade' COM(2021) 118 final.
[9] 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, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

from 250 to 750 employees, unless high-risk processing under Article 35 applies. Amendments to Articles 40(1) and 42(1) require that SMCs be formally considered in codes of conduct and certification schemes. While the reform signals a shift toward proportionality, critics warn that relaxed obligations could signal weakened data governance, and that voluntary instruments remain underutilised in practice. Still, the proposal may help ease the regulatory 'cliff effect' faced by SMEs moving to mid-cap status – though its impact will hinge on legislative outcomes and enforcement approaches.

2.1[b] Data Governance Act (DGA)

The Data Governance Act,[10] adopted on 30 May 2022, is the first of a series of legislative initiatives intended to create a European Single Market for data. It provides the legal foundation for the reuse of public sector data, data altruism mechanisms, and the establishment of trusted data intermediaries that enable secure and neutral data sharing across borders and sectors. The Act places significant emphasis on trust and neutrality, creating safeguards to prevent conflicts of interest and ensure the voluntary nature of data donations. Nevertheless, the DGA does not introduce climate-related use obligations for data intermediaries or processors, nor does it incorporate sustainability principles into data reuse governance. This is a missed opportunity: data reuse and processing efficiency could be incentivised on climate grounds, contributing to lifecycle optimisation and emissions tracking – objectives left untouched by the Act's design.

2.1[c] Digital Markets Act (DMA)

The Digital Markets Act,[11] adopted on 14 September 2022, introduces a novel ex ante competition framework aimed at correcting structural imbalances in the digital economy. It designates 'gatekeepers' – firms with entrenched intermediation power across core platform services – and imposes specific obligations and prohibitions to preserve market contestability and user autonomy. These include bans on self-preferencing, mandatory interoperability, and constraints on the bundling of services. However, the DMA's regulatory scope is entirely economic and behavioural. It does not address the carbon cost structures of gatekeepers, even though such actors operate large-scale cloud, AI and infrastructure services whose emissions and energy demands exceed those of some Member States. The omission of climate-related criteria – in an instrument that targets systemic actors in digital infrastructure – reinforces the segmentation of climate and digital law within the EU acquis.

[10] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) [2022] OJ L152/1.
[11] 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 and amending Directives (EU) 2019/1937 and 2020/1828 (Digital Markets Act) [2022] OJ L265/1.

2.1[d] Digital Services Act (DSA)

The Digital Services Act,[12] adopted on 19 October 2022, constitutes a major reform of the legal framework applicable to digital platforms, hosting services, and online intermediaries across the European Union. Its objectives are to ensure a safe, transparent, and accountable online environment, particularly by mitigating risks related to illegal content, disinformation, and algorithmic amplification. The DSA introduces binding due diligence obligations for 'very large online platforms' (VLOPs), including requirements for algorithmic transparency, systemic risk audits, and independent oversight. Importantly, these risks are narrowly defined in relation to societal harms such as electoral integrity, gender-based violence, or public health misinformation. The Act contains no provisions addressing the carbon footprint of platform infrastructure – such as energy-intensive content delivery networks, data storage, or algorithmic training pipelines – despite mounting evidence that platform operations contribute significantly to the digital sector's carbon emissions profile.

2.1[e] Data Act

The Data Act,[13] adopted on 13 December 2023, builds on the DGA and represents the EU's most ambitious attempt to regulate access to industrial data – especially data generated by Internet of Things (IoT) devices. It mandates that manufacturers and service providers make data accessible to users and empowers public authorities to request access in cases of exceptional public interest (e.g. natural disasters or public health emergencies). The Act is heralded as a milestone for horizontal data access rights and is expected to foster data-driven innovation, especially for SMEs and researchers. However, its climate-relevant potential remains unrealised. There are no explicit obligations to disclose or structure industrial data to support emissions tracking or resource optimisation. The Act treats data as an economic resource, not as a climate driver – a framing that reinforces the Union's prevailing data-as-commodity paradigm.

2.1[f] The AI Act

The AI Act, adopted on 13 June 2024, is the European Union's flagship regulatory framework for the development, placement on the market, and use of artificial intelligence systems. It establishes a risk-based regulatory model, classifying AI systems into four tiers – unacceptable risk (prohibited), high-risk (strictly regulated), limited risk (transparency obligations), and minimal risk (largely unregulated). High-risk systems, as defined in Annex III, are subject to mandatory conformity assessments, technical documentation requirements, human oversight, and post-market monitoring. The AI Act is widely seen as the world's first horizontal regulatory regime for AI, with extraterritorial reach and sectoral breadth. It emphasises human rights,

[12] 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) [2022] OJ L277/1.
[13] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data (Data Act) [2023] OJ L2023/2854.

safety, transparency, and trust – yet it omits any binding provisions on climate-compatible sustainability. Despite AI's growing resource and energy footprint, the Act contains no requirement to assess or disclose the climate impact of AI systems, even those requiring extensive computation or data processing. CE conformity assessments (Section 5 of the AI Act) do not include energy consumption, water use, or emissions as metrics of evaluation. As such, the AI Act typifies a regulatory model in which technological governance remains normatively detached from climate imperatives.

It should be noted that in February 2025, the European Commission adopted its first formal guidelines[14] interpreting the prohibitions under Article 5 of the AI Act, offering much-needed legal clarity on the scope and enforcement of unacceptable AI practices. These guidelines aim to ensure the uniform application of the Act's strictest rules, which prohibit AI systems deemed fundamentally incompatible with Union values and fundamental rights, including those that deploy subliminal manipulation, exploit vulnerabilities, conduct social scoring, or enable indiscriminate biometric surveillance. The document outlines how these prohibitions apply not only to AI providers but also to deployers, and clarifies that violations may trigger fines of up to €35 million or 7% of global turnover. Notably, the guidelines also articulate the non-exhaustive and contextual nature of these bans, emphasising the need for case-by-case assessments and offering illustrative examples of impermissible systems. These include AI-enabled emotion recognition at workplaces (except for medical or safety reasons), real-time remote biometric identification in public spaces by law enforcement (subject to narrow exceptions), and AI systems engaging in social scoring across domains. Importantly, while non-binding, the guidelines are a pivotal reference point for national authorities and practitioners navigating the early enforcement phase of the AI Act, and they reflect a broader regulatory intent: to defend human dignity and democratic integrity in an increasingly AI-mediated society. This interpretation represents the Commission's view as of the time of writing, and will evolve in response to emerging technologies and enforcement practice.

Taken together, the EU's digital legislative framework reveals a remarkable density, coherence, and ambition in structuring the digital internal market around values of transparency, accountability, competition, and fundamental rights. Through landmark instruments such as the GDPR, DGA, DMA, DSA, Data Act, and AI Act, the Union has constructed a far-reaching regulatory architecture capable of disciplining powerful platforms, securing data sovereignty, and asserting global normative leadership in emerging technologies. However, a shared structural omission persists across these initiatives: the systematic integration of climate mitigation and adaptation.

2.2 THE EU'S CLIMATE LEGISLATIVE FRAMEWORK: A HORIZONTAL OVERVIEW

Over the past decade, and especially since the launch of the European Green Deal[15] in 2019,

[14] European Commission, 'Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)' C(2025) 884 final.
[15] Commission, 'The European Green Deal' (n 2).

the European Union has pursued a far-reaching legislative agenda aimed at achieving climate neutrality. This legislative mobilisation – widely described as a green transformation – has resulted in an increasingly dense body of climate law, encompassing, inter alia, emissions trading and carbon border mechanisms. It reflects not only the urgency of the planetary crisis but also the Union's aspiration to lead the global transition toward climate neutrality.[16] Much like the digital rulebook, the climate acquis has evolved into a multi-instrumental and sectorally fragmented ecosystem, governed by a combination of regulations, directives, delegated acts, and policy communications.

2.2[a] EU Emissions Trading System (ETS)

The directive establishing the EU Emissions Trading System (ETS),[17] originally adopted on 13 October 2003, is the cornerstone of the Union's climate policy and its principal market-based instrument for reducing greenhouse gas emissions. It operates on a 'cap-and-trade' principle, setting a progressively declining cap on the total volume of emissions permitted from covered sectors – principally power generation, manufacturing, and aviation – with allowances traded on a regulated carbon market. Under the revised ETS framework, adopted in 2023 as part of the Fit for 55 package,[18] which is a comprehensive legislative package composed of multiple regulations and directives proposed and adopted to meet the EU's revised climate target of at least 55% net greenhouse gas emission reductions by 2030, the system was significantly expanded in scope and ambition: the cap will decline faster, free allowances will be gradually phased out, and a new ETS II will be introduced for road transport and buildings beginning in 2027. The revised directive also incorporates maritime transport and strengthens the Market Stability Reserve to control supply shocks. Revenues from the sale of allowances are earmarked for the Innovation Fund and Modernisation Fund, supporting green technology deployment and energy system upgrades across Member States. Despite its increasing sophistication, the ETS remains narrowly sectoral in design. Crucially, it does not cover emissions from digital infrastructures, including data centres, large-scale AI training operations, or the rapidly growing ICT sector more broadly. While these sources are becoming major contributors to electricity demand and lifecycle emissions in the EU, their climate impact falls outside the system's regulatory scope. In this sense, the ETS illustrates the EU's persistent failure to integrate digital sector emissions into its primary climate governance tools – an omission that undermines the Union's ability to internalise the full climate-related cost of its technological transformation.

[16] European Environmental Bureau, 'The European Green Deal – Knowledge Brief" (May 2025) <https://eeb.org/wp-content/uploads/2025/05/The-European-Green-Deal-Knowledge-Brief.pdf> accessed 22 August 2025.

[17] Directive 2003/87/EC of the European Parliament and of the Council of 13 October 2003 establishing a scheme for greenhouse gas emission allowance trading within the Community and amending Council Directive 96/61/EC (EU Emissions Trading System) [2003] OJ L275/32, as amended by Directive (EU) 2023/959 of the European Parliament and of the Council of 10 May 2023.

[18] European Commission, '"Fit for 55": Delivering the EU's 2030 Climate Target on the Way to Climate Neutrality' COM(2021) 550 final.

2.2[b] Effort Sharing Regulation (ESR)

The Effort Sharing Regulation (ESR),[19] first adopted in 2009 as a decision, and significantly revised in 2023 as part of the 'Fit for 55' package, is the EU's primary legislative instrument for governing greenhouse gas emissions in sectors not covered by the ETS, such as road transport, buildings, agriculture, and waste. The ESR sets binding annual emissions reduction targets for each Member State, based on GDP per capita and cost-efficiency criteria. The updated Regulation aims for a collective 40% emissions reduction by 2030, relative to 2005 levels, across these non-ETS sectors. It introduces stricter compliance mechanisms, increases transparency obligations, and expands the flexibility for Member States to trade emission allocations.[20] The ESR operates as a decentralised governance mechanism, empowering national governments to design and implement the policy mix needed to meet their obligations – ranging from subsidies and regulations to taxes and behavioural incentives. Despite its horizontal reach across many sectors of daily life, the ESR does not explicitly address emissions associated with digital infrastructures, even as these become increasingly embedded in transport, buildings, and service delivery. For example, emissions from the operation of cloud services in smart buildings or from digital logistics platforms in road freight fall outside the ESR's accounting logic. The Regulation reflects a conventional sectoral imagination that has yet to fully register the transversal character of digital technologies as both enablers and drivers of emissions. This blind spot reinforces the analytical and legal separation between the EU's digital and climate frameworks – an institutional legacy that hinders integrative climate policymaking.

2.2[c] The European Green Deal

The European Green Deal,[21] launched in December 2019, is the European Union's flagship political strategy for achieving climate neutrality, restoring biodiversity, and decoupling economic growth from environmental degradation. Presented as a transformative growth agenda, the Green Deal sets out a comprehensive policy roadmap spanning climate action, circular economy, energy efficiency, mobility, food systems, pollution control, and environmental justice. Its declared aim is to make Europe the world's first climate-neutral continent by 2050, while ensuring that the ecological transition is 'just and inclusive'.[22] Importantly, it must be underscored that the Green Deal is not a single legislative act, but rather a strategic framework that has triggered a cascade of regulatory initiatives and legislative proposals across virtually every policy domain. It functions as a meta-policy architecture, guiding the legislative priorities of the Commission and serving as the catalyst for an unprecedented wave of regulatory activity – including the European Climate Law, the 'Fit for 55' package,

[19] Regulation (EU) 2023/857 of the European Parliament and of the Council of 19 April 2023 on binding annual greenhouse gas emission reductions by Member States from 2021 to 2030 contributing to climate action to meet commitments under the Paris Agreement and amending Regulation (EU) 2018/842 (Effort Sharing Regulation) [2023] OJ L111/1.
[20] ibid Article 1.
[21] Commission, 'The European Green Deal' (n 2).
[22] ibid chapter 1 para 3; chapter 2.1.1 para 1.

the EU Taxonomy Regulation, and the Deforestation Regulation. It also initiated the Just Transition Mechanism and shaped key provisions in the Multiannual Financial Framework and Recovery and Resilience Facility. However, the Green Deal's operationalisation has revealed structural tensions: between economic competitiveness and ecological limits; between decarbonisation and biodiversity; and between rapid law-making and implementation capacity. Critically, while the Green Deal frequently invokes the digital transition as a complementary force, it stops short of articulating a coherent framework for governing the carbon footprint of digitalisation. This omission has allowed the digital and climate acquis to evolve along parallel but disconnected tracks, undermining the EU's ambition to deliver a truly integrated twin transition.

2.2[d] EU Taxonomy Regulation

The EU Taxonomy Regulation,[23] adopted in June 2020, establishes a common classification system to determine whether an economic activity can be considered environmentally sustainable. Designed to channel capital flows toward green investments and combat 'greenwashing', the Regulation defines six environmental objectives, including climate change mitigation and adaptation, sustainable use of water and marine resources, circular economy, pollution prevention, and biodiversity protection. To qualify as taxonomy-aligned, an activity must (i) contribute substantially to at least one of these objectives, (ii) do no significant harm (DNSH) to the others, and (iii) comply with minimum social safeguards. The Regulation serves as the foundation for other legislative initiatives, including the Sustainable Finance Disclosure Regulation (SFDR) and the Corporate Sustainability Reporting Directive (CSRD), and applies to financial market participants, large public-interest entities, and Member States developing green bond frameworks or sustainability labels. Despite its systematising ambition, the Taxonomy Regulation has faced significant political and technical challenges, including debates over the inclusion of nuclear energy and natural gas, delayed publication of delegated acts, and low uptake in actual financial reporting. More critically for this analysis, the taxonomy framework does not explicitly recognise the climate-specific sustainability of digital services or AI-related activities. Emissions from large-scale computing infrastructure, energy consumption in training foundation models, and e-waste from rapid device turnover fall outside its definitional core. As such, the Regulation reflects a conception of sustainability grounded in traditional industrial sectors, leaving the carbon footprint of digitalisation largely unclassified and unpriced. The lack of taxonomy criteria for digital operations also complicates the ability of firms to evaluate and disclose the sustainability of their digital value chains under the SFDR and CSRD – reinforcing the regulatory invisibility of the ICT sector's climate impact.

[23] Regulation (EU) 2020/852 of the European Parliament and of the Council of 18 June 2020 on the establishment of a framework to facilitate sustainable investment, and amending Regulation (EU) 2019/2088 (EU Taxonomy Regulation) [2020] OJ L198/13.

2.2[e] European Climate Law

The European Climate Law,[24] adopted on 30 June 2021, gives legal force to the political commitments articulated in the European Green Deal, transforming climate neutrality from a strategic ambition into a binding legal obligation. It establishes a Union-wide objective of achieving net zero greenhouse gas emissions by 2050,[25] and sets an intermediate binding target of a 55% reduction in net emissions by 2030, compared to 1990 levels.[26] The Regulation introduces a legal mechanism for tracking progress, requiring the Commission to periodically assess alignment with the climate neutrality trajectory and to issue recommendations or legislative proposals where Member States or EU law fall short.[27] It further mandates that all new Union-level policy initiatives must be assessed for their compatibility with the climate targets, and that both the Union and Member States are obliged to improve their climate adaptation strategies.[28] While normatively significant and institutionally binding, the Regulation is primarily architectural rather than operational: it provides an overarching legal framework but delegates implementation to sector-specific instruments such as the EU Emissions Trading System, the Effort Sharing Regulation, and carbon pricing reforms. Notably, the European Climate Law makes no reference to the climate impact of digital technologies, nor does it create accountability mechanisms for emissions associated with AI infrastructures, data centres, or ICT supply chains. It exemplifies the EU's vertical approach to climate governance – ambitious in scope, but still detached from the transversal dynamics of digitalisation.

2.2[f] Carbon Border Adjustment Mechanism (CBAM)

The Carbon Border Adjustment Mechanism (CBAM),[29] adopted in May 2023, represents a landmark development in EU climate policy, designed to address the risk of carbon leakage and preserve the integrity of the Union's climate ambitions. Operational from 2026, following a transitional phase, CBAM imposes a carbon price on certain imported goods – including cement, iron and steel, aluminium, fertilisers, hydrogen, and electricity – based on the emissions embedded in their production. Importers will be required to purchase CBAM certificates reflecting the carbon intensity of their products, unless they can demonstrate equivalent carbon pricing in the country of origin. The CBAM mirrors the EU ETS in methodology, and its pricing is indexed to the EU carbon market. It is the first mechanism of its kind globally, and signals the EU's willingness to externalise its climate disclosure standards to global trade partners under the principle of regulatory equivalence. While the CBAM is framed as a tool for fair competition

[24] Regulation (EU) 2021/1119 of the European Parliament and of the Council of 30 June 2021 establishing the framework for achieving climate neutrality and amending Regulations (EC) No 401/2009 and (EU) 2018/1999 (European Climate Law) [2021] OJ L243/1.
[25] ibid Article 2(1).
[26] ibid Article 4(1).
[27] ibid Articles 6(1)–(3).
[28] ibid Articles 7 and 5.
[29] Regulation (EU) 2023/956 of the European Parliament and of the Council of 10 May 2023 establishing a carbon border adjustment mechanism [2023] OJ L130/52.

and global decarbonisation, its design reveals a narrow focus on industrial commodities, with no provisions targeting digital goods, services, or infrastructures. Embedded emissions in imported electronics, AI-enabled hardware, or cloud-based computing services are not captured under the current scope. This exclusion reflects the broader disconnect between the EU's climate and digital regimes: even as the carbon intensity of imported ICT components rises, the environmental costs of digitalisation remain unpriced at the border. In this sense, CBAM exemplifies the EU's sectorally bounded approach to carbon regulation, which has yet to fully incorporate the climate externalities of digital trade.

It is to be noted that, despite its adoption and scheduled entry into its financial phase in January 2026, at the time of writing of this article CBAM is undergoing significant recalibration. In response to mounting industry pressure – particularly over the administrative complexity and financial burden associated with CBAM certificates – the European Commission has published a legislative proposal to amend the original Regulation. While reaffirming its commitment to the 2026 start date, the Commission has introduced a series of technical adjustments aimed at easing compliance and mitigating risk. Among the most consequential is a proposal to postpone the commencement of CBAM certificate sales until February 2027, due to unresolved issues with IT infrastructure. However, this does not amount to a deferral of financial obligations: importers will still be required to surrender certificates for emissions embedded in 2026 imports by August 2027. Additional reforms include raising the threshold for exempting small importers (now based on a 50-tonne net mass annually), extending declaration deadlines, and easing quarterly pre-purchase requirements from 80% to 50%. At the same time, the proposal significantly tightens enforcement, introducing fines of up to five times the value of unsurrendered certificates for deliberate non-compliance and establishing joint liability across supply chains in cases of circumvention.[30]

Taken as a whole, the EU's climate legislative framework constitutes an ambitious, densely layered architecture aimed at climate neutrality. Its instruments span carbon pricing, carbon taxation on imports entering the EU, CO^2 emission performance standards, etc. – together forming a powerful regulatory arsenal in response to accelerating planetary crisis. Yet, for all its depth and dynamism, this framework exhibits a striking structural feature: its persistent compartmentalisation. Despite frequent rhetorical nods to the 'twin transitions', the climate acquis remains technologically agnostic, failing to account for the climate impacts of the EU's digital transformation. Across nearly every major regulation – whether emissions trading, deforestation, or biodiversity recovery – digital infrastructures, AI systems, and computationally intensive technologies are treated as invisible actors, external to climate policy design. This normative detachment not only undermines the coherence of Union law but also renders key climate objectives less attainable in a world increasingly mediated by data and automation.

To conclude this Section, I turn to a critical reflection on the broader regulatory dichotomy

[30] Giovanni Gijsels and Tom Wallyn, 'The EU Proposes Sharper Carbon Border Rules: EC Proposes Key Amendments Ahead of the 2026 Definitive CBAM Phase' (*PwC News*, 4 March 2025) <https://news.pwc.be/the-eu-proposes-sharper-carbon-border-rules-ec-proposes-key-amendments-ahead-of-the-2026-definitive-cbam-phase/> accessed 1 September 2025.

that has emerged between the European Union's digital and climate legislative frameworks. As I have argued throughout, these two agendas – though rhetorically presented as 'twin transitions' – remain institutionally and normatively disconnected. I am a firm proponent of a holistic and complementary approach that recognises the interdependence of digital infrastructures and climate resilience. Only by embedding climate objectives into digital governance, and vice versa, can the Union align innovation with its constitutional commitment to climate neutrality. This vision is well captured by President Charles Michel, who stated in a 2021 speech to the European University Association: 'This holistic approach will not only power our climate and digital ambitions, it will generate economic prosperity and shore up our resilience'.[31] His words are not just aspirational – they offer a blueprint for legal coherence in a time of intersecting systemic crises. Holistic thinking, in this context, is not optional: it is a structural necessity if the EU is to fulfil its dual ambitions of technological leadership and planetary stewardship.

3 NEGOTIATED AWAY: CLIMATE INTEGRITY AND THE POLITICS OF THE AI ACT

While the AI Act has been hailed as a landmark in global technology governance, its final shape reflects not only normative ambition, but also the structural realities of European Union law-making – where competing interests are not peripheral but structurally embedded into the legislative process itself. The EU's supranational configuration, with its multi-layered institutional architecture and co-decision procedures, inevitably generates legislative outcomes shaped by negotiation, compromise, and sectoral balancing. In this context, inter-service rivalries, political trade-offs, and lobbying influence are not aberrations, but rather systemic features of EU governance. This Section examines how climate considerations – initially present in early drafts and interdepartmental consultations – were ultimately excluded or diluted through a combination of bureaucratic streamlining, legislative compromise, and industry pressure. Drawing on documented trilogue negotiations, stakeholder submissions, and critical policy analysis, the Section traces the mechanisms through which climate provisions were deprioritised, particularly within the European Commission's internal structure. It contends that the absence of climate-related safeguards in the AI Act is not merely an oversight, but the outcome of procedural dynamics that systematically privilege market and rights-based concerns over climate mainstreaming. Understanding these legislative peripeteia is essential to evaluating the Act's regulatory integrity – and to imagining a future revision that aligns technological governance with the Union's climate commitments.

[31] Charles Michel, 'Speech by President Charles Michel at the European University Association Annual Conference' (*Parlementaire Monitor*, 22 April 2021) <https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vli6i7aeziz8?ctx=vhsih95vppua&tab=1> accessed 1 September 2025.

3.1 BALANCING CLIMATE AMBITION WITH STAKEHOLDER CONCERNS

The evolution of the AI Act illustrates the broader challenge of integrating climate objectives into complex regulatory frameworks shaped by multi-actor negotiations, competing priorities, and economic sensitivities. This tension is particularly evident in the treatment of climate provisions during the legislative process. Throughout the legislative negotiations surrounding the AI Act, the European Parliament's Committee on the Environment, Public Health and Food Safety (ENVI) advanced several proposals intended to strengthen the climate dimension of the regulation.[32] Among these were amendments calling for energy efficiency standards in AI system design and the promotion of sustainability practices in data centre operations. These initiatives reflected a growing recognition of the climate externalities associated with AI infrastructures, particularly in terms of energy intensity and resource use. However, many of these proposals did not find their way into the final legislative text. Available evidence suggests that concerns raised by industry stakeholders – particularly regarding innovation capacity, regulatory complexity, and global competitiveness – played a role in shaping the outcome of the trilogue negotiations and the overall regulatory compromise.

The adopted version of the Act includes a limited climate reference in Article 40(2), which obliges the Commission, when issuing standardisation requests, to ensure that they also cover energy and resource efficiency, including requirements on the lifecycle energy consumption of high-risk AI systems and the energy-efficient development of general-purpose AI models.[33] While this provision signals an awareness of climate implications, its scope remains relatively narrow, and it does not impose specific targets or obligations related to emissions and resource efficiency. As a result, some scholars and policy commentators have expressed concern that the AI Act, in its current form, may not fully reflect the climate dimensions of digital transformation. Rather than an intentional omission, this may reflect broader structural dynamics within the EU's legislative process, where competing regulatory priorities and institutional mandates often require complex and politically sensitive trade-offs.

3.2 CORPORATE CAPTURE AND THE REGULATORY SCOPE OF THE AI ACT

The legislative trajectory of the AI Act illustrates a broader pattern of corporate influence on digital regulation, often characterised in the academic literature as corporate capture. In this context, large technology companies – including OpenAI, Microsoft, and Google – played a significant role in shaping key provisions of the Act, particularly those related to the

[32] Committee on the Environment, Public Health and Food Safety, 'Opinion for the Committee on the Internal Market and Consumer Protection and for the Committee on Civil Liberties, Justice and Home Affairs on the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts' COM(2021) 0206 final, C9-0146/2021, 2021/0106(COD) (25 January 2022), PE699.056v01-00, Rapporteur: Susana Solís Pérez <https://artificialintelligenceact.eu/wp-content/uploads/2022/05/AIA-ENVI-Rule-56-Opinion-Adopted-22-April.pdf> accessed 1 September 2025.

[33] Green Software Foundation, 'The EU AI Act: Insights from the Green AI Committee' (*Green Software Foundation*, 23 April 2024) <https://greensoftware.foundation/articles/the-eu-ai-act-insights-from-the-green-ai-committee> accessed 1 September 2025.

classification and obligations of advanced AI systems. These actors engaged intensively with European policymakers throughout the legislative cycle, advocating for regulatory frameworks that would preserve operational flexibility and minimise compliance burdens.[34]

A notable instance of this influence concerns the treatment of general-purpose AI models. OpenAI, for example, lobbied against the categorisation of its systems as 'high-risk', which would have triggered extensive oversight obligations, potentially including climate impact assessments. This lobbying contributed to the creation of a distinct regulatory tier for 'foundation models', which, while subject to certain transparency and risk management obligations, fall outside the strictest regulatory framework of the Act. The reclassification of these systems has important implications not only for safety and accountability, but also for climate governance: the lighter regulatory touch afforded to foundation models means that potential climate resilience assessments tied to risk-based obligations were effectively circumvented. As such, the episode reflects a structural feature of EU law-making, where concentrated private sector engagement may shape legislative boundaries – sometimes to the detriment of broader climate or public interest considerations.

3.3 MEMBER STATE DISAGREEMENTS AND NATIONAL INTERESTS

During the negotiation and adoption of the EU AI Act, internal disagreements among Member States, particularly Germany, France, and Italy, significantly influenced the shaping of the legislation's provisions. These countries expressed concerns that stringent regulations could hinder innovation and economic growth, leading to a push for more flexible approaches.

In November 2023, Germany, France, and Italy reached a joint agreement on the future of AI regulation in Europe. This agreement emphasized the need for voluntary commitments that would be binding for both small and large AI providers within the EU. The three governments advocated for rules of conduct and transparency to be binding for all, suggesting that initial sanctions should not be imposed but could be considered if violations occur after a certain period. This stance was seen as a move to balance regulation with competitiveness, aiming to foster innovation while ensuring responsible AI adoption. Furthermore, these countries opposed certain provisions related to the regulation of foundation models, arguing that overly strict rules could stifle innovation and economic growth.[35] Their position contributed to the dilution of some climate-related requirements in the final legislation. The concerns raised by Germany, France, and Italy were eventually addressed, leading to a unanimous vote on 2 February 2024 by all 27 EU Member States at the Council of the European Union to approve the latest draft of the AI Act. This resolution signalled a consensus that balanced the need for regulation with the imperative to support innovation across the EU.

These developments highlight the complex interplay between regulatory ambitions and

---

[34] Billy Perrigo, 'OpenAI Secretly Lobbied the EU to Water Down AI Rules' (*Time*, 14 June 2023) <https://time.com/6288245/openai-eu-lobbying-ai-act/> accessed 1 September 2025.

[35] Amnesty International, 'EU: France, Germany and Italy Risk Unravelling Landmark AI Act Negotiations' (*Amnesty International*, 27 November 2023) <https://www.amnesty.org/en/latest/news/2023/11/eu-france-germany-and-italy-risk-unravelling-landmark-ai-act-negotiations/> (accessed 1 September 2025.

national interests within the EU, illustrating how internal disagreements can shape the trajectory of significant legislative initiatives like the AI Act.

3.4 CIVIL SOCIETY PARTICIPATION IN EU AI GOVERNANCE: SCOPE, LIMITS, AND IMPLICATIONS

The negotiation and adoption of the AI Act demonstrated the structural challenges civil society organizations, particularly those focused on climate mitigation and adaptation, face in influencing high-stakes digital regulation. Although the Act acknowledges the potential climate ramifications of artificial intelligence technologies, civil society's limited access to the legislative process and comparatively modest resources hindered the incorporation of robust climate clauses in the final text.

Access to key decision-making venues during the legislative process was highly asymmetrical. Industry actors, particularly major technology firms, maintained consistent and well-organized engagement with EU institutions through structured consultations, bilateral meetings, and dedicated lobbying. In contrast, many civil society organizations, including climate advocacy organisations, encountered difficulties in gaining visibility within these channels. This access gap limited their ability to present expertise in climate action or advocate for more binding climate policy safeguards during critical phases, such as the trilogue negotiations.

Resource asymmetries further compounded this challenge. In 2024, the top 50 technology companies spent over €200 million on lobbying efforts in Brussels, enabling sustained and technically detailed contributions to the regulatory process. Civil society, by contrast, relies on significantly smaller budgets. The EU's LIFE Programme – the primary mechanism for supporting climate NGOs – allocates approximately €15.6 million annually across the entire Union. Moreover, recent changes to funding eligibility rules restrict the use of EU funds for advocacy activities, further constraining civil society's ability to intervene effectively in policymaking arenas.[36]

Despite these limitations, civil society actors submitted detailed proposals aimed at integrating concrete climate requirements into the AI Act. The Act does include a limited requirement for energy consumption reporting, applicable to general-purpose AI models. Yet, this provision does not extend to broader indicators such as greenhouse gas emissions, resource intensity, or material lifecycle impacts. As such, the climate dimension of AI governance in the EU remains underdeveloped.[37] National preferences also influenced the final outcome. Several large member states – such as Germany, France, and Italy – advocated for a proportionate regulatory framework that would preserve flexibility and competitiveness. Their position contributed to the softening of certain requirements, including those related to climate neutrality, and shaped a consensus that emphasized innovation-friendly governance.

---

[36] The Good Lobby, 'The End of NGO Advocacy in Europe? New EU Funding Restrictions Threaten Environmental NGOs' (*The Good Lobby*, 29 January 2025) <https://thegoodlobby.eu/the-end-of-ngo-advocacy-in-europe-new-eu-funding-restrictions-threaten-environmental-ngos/> accessed 1 September 2025.

[37] José Renato Laranjeira de Pereira, 'The EU AI Act – A Missed Opportunity?' (*Heinrich Böll Foundation EU Office*, 8 April 2024) <https://eu.boell.org/en/2024/04/08/eu-ai-act-missed-opportunity> accessed 1 September 2025.

Looking ahead, a number of philanthropic and civil society actors have called for reforms to strengthen participatory governance in EU digital regulation. These include institutional mechanisms to guarantee meaningful consultation with NGOs, transparent lobbying registers, and targeted funding to support public interest engagement. Such measures may help redress the current imbalance and ensure that future digital legislation is more inclusive of climate and societal concerns.

3.5 OPAQUE DYNAMICS AND POLITICAL BARGAINING IN THE EU AI ACT

The legislative odyssey of the EU AI Act also offers a revealing case study in the politics of digital regulation within multilevel governance. Beneath the formal narrative of interinstitutional compromise lies a more complex story – one made partially visible through leaked drafts, prolonged deadlocks, and the strategic opacity of the trilogue process. These unofficial disclosures, while technically outside formal procedural channels, have provided crucial insights into how the normative architecture of the Act was contested, reinterpreted, and ultimately diluted.

The January 2024 leak of the so-called 'final consolidated draft' marked a pivotal moment in understanding the inner workings of AI Act negotiations.[38] This draft, circulated ahead of official publication, contained hybrid language reflecting concessions made between the European Commission, the Council, and the European Parliament. It exposed not only how central concepts – such as the definitions of 'general-purpose AI models' and 'high-risk systems' – were evolving under institutional pressure, but also how core regulatory obligations were being subtly eroded or reworded to secure political consensus. Legal scholars and civil society actors noted that the language in the draft often mirrored lobbying preferences voiced by dominant Member States and industry actors, particularly with respect to the classification thresholds and enforcement flexibility granted to providers of foundation models.

More revealing still was the protracted impasse over the regulation of biometric identification systems, especially remote facial recognition technologies. In December 2023, trilogue negotiations reportedly extended over 22 hours without agreement, with lawmakers deadlocked over the inclusion of narrow public security exemptions versus broader fundamental rights protections.[39] The biometric debate served as a microcosm of deeper unresolved tensions between national security prerogatives and the EU's own Charter-based commitments to privacy, non-discrimination, and human dignity. Member States such as France and Germany reportedly lobbied for greater leeway for national police forces, while Parliament rapporteurs pushed for categorical bans on real-time facial recognition in public spaces. The resulting compromise – allowing certain uses with judicial authorization – was criticized by digital rights groups as a regression from earlier parliamentary ambitions.

---

[38] Hunton Andrews Kurth LLP, 'Final Draft of EU AI Act Leaked' (*Privacy and Information Security Law Blog*, 1 February 2024) <https://www.hunton.com/privacy-and-information-security-law/final-draft-of-eu-ai-act-leaked> accessed 1 September 2025.

[39] Gian Volpicelli, 'AI Act Negotiations Enter Their 19th Hour' (*Politico Europe*, 7 December 2023) <https://www.politico.eu/article/ai-act-negotiations-enter-their-19-hour/> accessed 1 September 2025.

These events prompted a growing chorus of concern over the opacity of the trilogue process. Unlike ordinary committee proceedings, trilogues are closed-door negotiations, shielded from real-time public or stakeholder scrutiny. The leaks, then, functioned less as procedural breaches than as de facto transparency mechanisms – exposing not only the fragility of interinstitutional consensus but also the political asymmetries shaping Europe's flagship digital legislation.[40] The piecemeal and reactive nature of compromise that emerged under these conditions points to a broader institutional pathology: the tendency of EU digital governance to sacrifice normative coherence for speed and symbolic leadership on the global stage.

From a rule-of-law and democratic legitimacy perspective, the procedural irregularities – while not unlawful – raise valid questions about accountability in the shaping of high-stakes technological norms. The AI Act was widely promoted as a rights-based framework. Yet, as the leaked documents suggest, some of its most consequential provisions were brokered away in forums inaccessible to public oversight, often in response to pressure from both Member States and industry stakeholders concerned with competitiveness and administrative burden. The final regulation thus risks reflecting not the EU's normative ambitions, but the constraints of its procedural pragmatism.

The foregoing analysis suggests that, viewed within its full official and off-the-record context, the legislative trajectory of the AI Act underscores a deeper insight into the structural logic of EU law-making – one shaped less by grand normative declarations than by what may be termed procedural realism. The Act's final configuration did not result from a simple failure of political will, but rather from the embedded dynamics of a system that prioritises compromise, administrative feasibility, and market stability. Throughout its gestation, the Act was filtered through layers of interinstitutional bargaining, national positioning, and asymmetrical stakeholder access – mechanisms that, while formally legitimate, systematically constrained the integration of climate-related exigencies. What ultimately emerged is a regulation fluent in the grammar of risk, rights, and innovation, yet markedly reticent when it comes to climate – a silence not incidental, but structured.

4 MAPPING THE CLIMATE BLIND SPOT IN THE AI ACT

This Section undertakes a systematic exploration of the structural omissions and regulatory lacunae that characterise the AI Act in its treatment – or, more precisely, its neglect – of climate considerations. Although the Act has been widely acclaimed as a global benchmark for responsible AI governance, its internal architecture fails to meaningfully embed climate metrics or mandatory energy-efficiency obligations. This shortcoming is particularly noteworthy in the context of the European Union's own policy rhetoric, which consistently frames the digital and green transitions as interdependent vectors of the Union's strategic future.

Having thus far laid the doctrinal and institutional groundwork in the preceding

[40] Jedidiah Bracy, 'EU AI Act Draft Consolidated Text Leaked Online' (*International Association of Privacy Professionals*, 22 January 2024) <https://iapp.org/news/a/eu-ai-act-draft-consolidated-text-leaked-online> accessed 1 September 2025.

Sections – tracing both the expansive digital legislative framework and the fragmented climate acquis – it is now time to delve into the regulatory substrata of the AI Act itself. This Section turns to the textual and structural anatomy of the legislation to identify where, how, and to what extent climate considerations were side-lined in favour of more narrowly construed policy goals. What follows is a granular examination of specific provisions – Annexes, Articles, and institutional instruments – through which the Act operationalises its risk-based model. In so doing, we expose the precise legal and procedural locations in which the climate dimension was either omitted, deprioritised, or rendered legally inert.

4.1 ABSENCE OF CLIMATE RISK IN HIGH-RISK CATEGORIES (ANNEX III)

The cornerstone of the AI Act's regulatory architecture is its risk-based classification system, whereby AI systems are stratified into risk tiers – ranging from 'unacceptable risk' (prohibited) to 'high-risk' (strictly regulated), 'limited risk' (transparency obligations), and 'minimal risk' (largely unregulated). Central to this structure is Annex III, which exhaustively enumerates the categories of AI applications deemed to pose a 'high risk' to fundamental rights, health, and safety. These include biometric identification systems, AI in critical infrastructure, educational and employment systems, credit scoring, law enforcement tools, and systems used in migration and border control.

Yet, conspicuously absent from this taxonomy is any mention of climate risk. Neither carbon emissions, energy intensity, water usage, nor any other climate externality is considered in the determination of high-risk AI systems. This omission is not merely semantic; it is structurally embedded. The legislative text makes no provision for categorising AI systems as high-risk on the basis of their carbon footprint – despite the growing body of evidence on the energy demands of training large-scale AI models and the climate costs of AI-driven infrastructures such as data centres and edge computing systems.

This lacuna is particularly striking given the Union's own rhetorical and policy emphasis on the so-called twin transitions – the simultaneous pursuit of digital and green transformation. If the climate effects of AI systems are not accounted for at the threshold stage of risk classification, then the regulatory framework that follows – conformity assessments, CE marking, post-market monitoring – will also remain climate-wise blind. The absence of climate-related triggers in Annex III thus represents not only a technical oversight but a normative misalignment between the AI Act and the Union's broader climate acquis.

As some scholars have noted, this exclusion risks creating a two-tier governance model in which AI systems with social or human rights risks are subject to oversight, while those with climate implications are effectively exempted from regulatory scrutiny.[41] This is especially troubling given the increasing use of AI in sectors with high climate externalities, such as energy optimisation, industrial automation, and digital agriculture.

Unless and until Annex III is updated to include climate risk categories – whether based on absolute energy thresholds or emissions benchmarks, – the AI Act will remain structurally

[41] Laranjeira de Pereira (n 37).

unfit to address one of the most pressing dimensions of contemporary technological governance: the climate neutrality of artificial intelligence.

4.2 NO LIFECYCLE EMISSIONS OR ENERGY TRANSPARENCY IN TECHNICAL DOCUMENTATION (ANNEX IV)

Annex IV of the EU AI Act outlines the technical documentation requirements for high-risk AI systems, serving as a cornerstone for the conformity assessment process. However, it notably lacks explicit criteria or obligations pertaining to climate integrity.

Specifically, Annex IV mandates that providers furnish comprehensive details about the AI system's intended purpose, design specifications, data management practices, and risk management strategies. While these requirements encompass aspects such as human oversight, accuracy, robustness, and cybersecurity, they do not address the climate impacts associated with AI systems, such as energy consumption during training and deployment or the carbon footprint of hardware production. This omission is particularly concerning given the substantial carbon footprint of AI technologies. Scholars have highlighted that the AI Act fails to account for the energy consumed during the inference phase of AI operations, which can be significant. This oversight means that a substantial portion of AI's climate impact is not subject to regulatory scrutiny.[42] Furthermore, while the AI Act's recitals acknowledge the importance of climate change mitigation (cf. recitals 40 and 130), these considerations are not translated into binding obligations within the conformity assessment framework. The reliance on voluntary codes of conduct and deferred standardization processes lacks the enforceability needed to ensure that AI systems align with the EU's climate objectives, such as those outlined in the European Green Deal.

In conclusion, the current structure of Annex IV and the broader conformity assessment procedures under the EU AI Act do not adequately integrate climate sustainability criteria. This gap underscores the need for the development of harmonized standards or amendments to the existing framework to ensure that AI systems contribute positively to the EU's climate goals.

4.3 NO CARBON ACCOUNTING STANDARDS IN CONFORMITY ASSESSMENT PROCEDURES

The conformity assessment procedures embedded in the AI Act are designed to ensure that high-risk AI systems comply with the essential requirements set out in Chapter III of the Regulation. These procedures serve as a gatekeeping mechanism, certifying that an AI system adheres to standards related to safety, transparency, robustness, and accountability before it may be placed on the Union market. However, a close reading of Articles 43-51 and Annexes VI–IX reveals a fundamental lacuna: these conformity procedures do not mandate or even encourage the assessment of climate-related risks.

The AI Act outlines a comprehensive process through which high-risk systems are subject

[42] Kai Ebert et al, 'AI, Climate, and Regulation: From Data Centers to the AI Act' (*SSRN*, 22 November 2024) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4980340> accessed 1 September 2025.

to ex ante scrutiny, either through internal control or third-party assessments, depending on whether the AI system is covered by harmonised standards. Yet, none of the conformity pathways require providers to evaluate the carbon footprint of the AI systems, including dimensions such as carbon intensity, energy consumption, or the ecotoxicity of hardware supply chains. This is a striking omission given the growing body of evidence demonstrating the climate impact of large-scale AI training and inference models.

From a regulatory design perspective, this exclusion suggests a narrow technocratic conception of risk, limited primarily to social harms and human safety. The climate dimension of AI, by contrast, remains external to the assessment architecture. This disconnect is particularly problematic when considered alongside parallel EU legislation. As the European Commission explains in the Sustainable Products Initiative,[43] 'Consumers, the environment and the climate will benefit from products that are more durable, reusable, repairable, recyclable, and energy-efficient'. In the same vein, the Ecodesign for Sustainable Products Regulation,[44] empowers the Commission to adopt delegated acts establishing product-specific requirements on climate performance, including carbon footprint (Article 5(1)(o) and imposes a sensitivity analysis covering the avoided greenhouse gas emissions (Annex II, para 8). Similarly, the Corporate Sustainability Reporting Directive (CSRD),[45] provides that the sustainability reporting standards have to specify information that the undertakings are to disclose about climate change mitigation and climate change adaptation (Article 29b(2)(a)(i)–(ii)). Taken together, these instruments embed climate considerations directly into compliance structures, ensuring that greenhouse gas emissions are monitored, reported, and progressively reduced both at the level of products and of corporate governance.

The AI Act, in contrast, embeds no such requirement at the level of regulatory procedure, even for AI systems known to incur substantial energy demands or climate-related costs. Moreover, the lack of integration with the EU Taxonomy Regulation – which expressly establishes climate change mitigation and adaptation as two of its central objectives (Articles 10 and 11) – further isolates the AI Act from the Union's broader climate governance. This divergence is not only normative but operational: firms subject to both AI compliance obligations and climate reporting may be forced to navigate two parallel compliance regimes, one climate-wise agnostic and the other climate-forward.

In effect, the conformity assessment regime reinforces the AI Act's climate blindness at the procedural level. Without explicit metrics, thresholds, or requirements concerning climate-linked performance, the AI compliance system provides no regulatory incentive for

[43] European Commission, 'Sustainable Products Initiative' (*Have Your Say Europe*, webpage) <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12567-Sustainable-products-initiative_en> accessed 1 September 2025.
[44] Regulation (EU) 2024/1781 of the European Parliament and of the Council of 13 June 2024 establishing a framework for the setting of ecodesign requirements for sustainable products, amending Directive (EU) 2020/1828 and Regulation (EU) 2023/1542 and repealing Directive 2009/125/EC [2024] OJ L2024/1781.
[45] Directive (EU) 2022/2464 of the European Parliament and of the Council of 14 December 2022 amending Regulation (EU) No 537/2014, Directive 2004/109/EC, Directive 2006/43/EC and Directive 2013/34/EU, as regards corporate sustainability reporting [2022] OJ L322/15.

sustainable AI system design or lifecycle optimisation. As some scholars have observed,[46] this procedural lacuna is not incidental but symptomatic of the sectoral fragmentation of EU regulatory governance, in which digital innovation and decarbonisation pathway are governed on divergent tracks.

4.4 REGULATORY SANDBOXES AND THE ABSENCE OF CLIMATE FILTERS

While the AI Act introduces a novel mechanism to foster innovation – AI regulatory sandboxes – these experimental zones fall short of addressing the European Union's climate neutrality objectives. Codified in Articles 57 to 61 of the AI Act, regulatory sandboxes are controlled environments where providers and prospective providers can test AI systems before deployment, under the supervision of national competent authorities. However, a close textual analysis reveals a conspicuous omission: the absence of any explicit obligation or framework to assess or promote climate neutrality within these sandboxes.

Despite Recital 139 emphasising that sandboxes are intended to support 'regulatory learning' and facilitate 'compliance of the innovative AI systems with this Regulation and other relevant Union and national law' the operative provisions make no mention of climate neutrality. Instead, the regulation concentrates on fundamental rights, safety, and data protection, delegating oversight of those domains to relevant authorities. In Article 57(6), for instance, competent authorities are instructed to supervise for risks to fundamental rights, health, and safety – but not climate resilience. This lacuna persists even in Article 58, which mandates the Commission to adopt implementing acts detailing the sandbox framework. While this article provides principles for accessibility, resource allocation, and conformity assessment, it does not incorporate climate-related standards or even general climate-linked criteria as conditions for participation or evaluation. The oversight is all the more striking in light of proposals from the European Parliament during earlier negotiations, which sought to prioritise access to sandboxes for projects demonstrating climate mitigation value. These suggestions, however, were not adopted in the final version. An exception exists in Article 59, which allows for further processing of personal data within regulatory sandboxes for projects serving substantial public interest. Notably, this includes development in areas such as climate change mitigation and green transition. Yet, this clause is narrowly scoped to data processing and does not translate into broader climate-related performance criteria across sandbox operations.[47]

Consequently, the regulatory sandbox framework represents a missed opportunity to embed climate consciousness in early-stage AI experimentation. Without climate filters or climate impact assessments, sandboxes may inadvertently incentivise the development of energy-intensive, ecologically detrimental AI systems under the banner of innovation. As such,

---

[46] Sara Garsia, 'The environmental costs of AI: a shake-up of the EU's twin transition' (*Law, Ethics & Policy of AI Blog*, 28 February 2025) <https://www.law.kuleuven.be/citip/blog/the-environmental-costs-of-ai-a-shake-up-of-the-eus-twin-transition/> accessed 1 September 2025.

[47] Davide Baldini and Kate Francis, 'AI Regulatory Sandboxes Between the AI Act and the GDPR: The Role of Data Protection as a Corporate Social Responsibility' (CEUR Workshop Proceedings vol. 3731, 2024) <https://cris.maastrichtuniversity.nl/en/publications/ai-regulatory-sandboxes-between-the-ai-act-and-the-gdpr-the-role-> accessed 1 September 2025.

integrating mandatory climate considerations into sandbox eligibility criteria, project evaluation, and supervision mechanisms could form a crucial next step in aligning innovation support instruments with the Union's climate agenda.

4.5 MISSED OPPORTUNITY FOR CLIMATE-SENSITIVE AI BY DESIGN

Despite the growing recognition of the role that design-phase decisions play in determining the long-term climate ramifications of technologies, the AI Act omits any formal requirement for 'climate-sensitivity by design' in the architecture, training, or deployment of artificial intelligence systems. Chapter III of the Regulation, on the high-risk AI systems – delineating requirements on risk management, data governance, technical documentation, and human oversight, etc. – are focused almost exclusively on safeguarding health, safety, fundamental rights, and cybersecurity. Thus, climate awareness is not treated as regulatory priority in the AI Act.

Analogously, this omission is particularly striking given the increasing policy emphasis on sustainability by design in adjacent EU legislative instruments, such as the Ecodesign for Sustainable Products Regulation (Regulation (EU) 2024/1781). In the context of AI, such a principle would require developers to evaluate and mitigate climate-related harms, including greenhouse gas emissions at the earliest stages of system development. However, the AI Act does not include such mandates into its core compliance architecture.

Scholarship explicitly advocating the adoption of climate impact assessments (CIAs) for artificial intelligence remains at an incipient stage. Such an assessment would encompass both the adverse effects of AI on the climate – chiefly arising from energy consumption and emissions embedded in hardware manufacturing – and its positive potential to contribute to climate mitigation by optimising energy systems, advancing clean technologies, and enabling the monitoring of climate phenomena. Emerging frameworks for evaluating AI's net impact underscore that its contribution can be overwhelmingly beneficial, provided it is deliberately steered towards accelerating low-carbon transitions, while complementary policies are developed to contain and redress its negative externalities. A salient illustration is the written submission by the community-based organisation Climate Change AI in response to the Request for Information on National Priorities for Artificial Intelligence.[48] The submission underscores that AI has significantly accelerated emissions-intensive industries while also driving broader systemic transformations – such as heightened consumption, shifts in information dissemination, the entrenchment of individualised mobility through autonomous vehicles, and accompanying redistributions of social power – that collectively impede progress towards climate objectives. On this basis, it contends that climate change must constitute a central criterion in shaping not only 'AI for good' initiatives but the development of AI applications more generally. To this end, the organisation advocates the deployment of policy levers including: the mandatory integration of climate impact assessments into the evaluation of AI projects deemed strategic; the avoidance of direct public funding for AI applications that

[48] Climate Change AI, Priya L Donti, David Rolnick, Jade E Guisiano, Sara Beery, Lynn Kaack and Sebastian Ruf, Climate Change AI (7 July 2023) <https://downloads.regulations.gov/OSTP-TECH-2023-0007-0274/attachment_1.pdf> accessed 25 October 2024.

contravene climate objectives; and the imposition of reporting and accountability obligations on organisations for the emissions attributable to AI.

The legislative negotiations on the AI Act unfolded as a theatre of competing interests. They reveal,[49] for instance, that the Commission's original proposal did not embed climate risk in the core risk taxonomy or essential requirements; instead, MEPs in ENVI tried to graft climate-specific duties onto the text through add-ons flagging AI's carbon footprint and urging minimisation of climate impacts, and criteria tying 'high-risk' classification to adverse effects on the climate and on meeting EU greenhouse-gas targets. They proposed hard obligations to measure and disclose lifecycle energy use and GHG emissions, to log energy/resource use and GHGs, and to include energy-consumption and carbon-intensity information in technical documentation and even a visible energy/carbon label. ENVI also tabled a 'proportionality framework' to halt model training where the projected carbon footprint outweighed benefits and suggested periodic Commission reviews geared to decarbonising AI technologies by 2050 – all explicitly climate-centred in their nature. Ultimately, climate safeguards (carbon metrics, labels, climate-conditioned risk triggers) surfaced mainly as amendments – recitals, new articles, and annexes appended to a market/safety/fundamental-rights instrument – rather than as structural elements of the baseline proposal. These drafting choices illustrate that the climate perspective was pushed to the margins of the negotiation text, addressed through peripheral compliance add-ons rather than integrated into the Act's core architecture.

In the same vein, proposals for sustainability by design were not absent from the legislative debate. Certain amendments proposed during the European Parliament's deliberations sought to introduce environmental risk assessment requirements for both high-risk AI systems and foundation models. However, these proposals were not retained in the final version of the Regulation. This suggests a broader pattern in which environmental and climate-linked concerns were treated as ancillary rather than integral to the risk framework.[50]

Thus, the AI Act's current architecture misses a critical opportunity to institutionalize climate-sensitive AI by design at the heart of AI governance. This omission limits the EU's ability to ensure that its digital and green transitions advance in concert rather than in conflict. If left unaddressed, it risks embedding climate-wise suboptimal practices into the rapidly proliferating landscape of AI development.

These regulatory omissions do not merely reflect a technical oversight – they underscore a broader disjunction between the EU's AI governance framework and its long-term strategic objectives. By failing to fully account for the climate-related externalities of AI development, the Union risks advancing digital innovation at the expense of its climate commitments. As noted by the Harvard Ash Center,

> The EU must also consider how AI investments may conflict with its other long-term objectives. For example, while AI has the potential to make processes more efficient, it can also contribute to environmental degradation due to the energy demands of

[49] Amnesty International (n 35), Volpicelli (n 39).
[50] Anna Aseeva, 'Liable and Sustainable by Design: A Toolbox for a Regulatory Compliant and Sustainable Tech' (2024) 16(1) Sustainability 228.

> large-scale data centers and the environmental footprint of hardware production, undermining the European Green Deal and climate neutrality goals. AI-driven automation could also lead to job displacement, exacerbating inequality and weakening the EU's social cohesion and vision of an 'economy that works for people.[51]

This observation highlights the need for a governance approach that is not merely risk-based, but integrative – one that aligns AI deployment with Europe's green ambitions.

The preceding analysis has demonstrated that, despite its celebrated ambition and granularity in addressing algorithmic risks, the AI Act consistently falls short in integrating climate considerations across its core regulatory pillars. From the absence of climate risks in the high-risk classification schema (Annex III), to the lack of climate metrics in technical documentation (Annex IV), conformity assessments, and provider obligations, the climate dimension remains peripheral – if not entirely invisible. Regulatory sandboxes, touted as innovation-friendly instruments, likewise neglect climate-related criteria, while the omission of climate-sensitive AI by design forecloses structural incentives for climate-responsible AI development. What emerges is not simply a set of isolated exclusions, but a pattern of regulatory lacunae that systematically sideline the climate change implications of AI. This regulatory architecture reflects a deeper policy disjunction between the EU's digital and green agendas – agendas that are politically interlinked but legislatively estranged. Bridging this gap requires more than rhetorical convergence; it calls for targeted amendments designed to embed climate accountability throughout the entire AI lifecycle.

5 TOWARDS CLIMATE-CONSCIOUS EU AI REGULATION – POLICY RECOMMENDATIONS AND LEGAL PATHWAYS

The most rigorous critique, as jurists often observe, is not one that dismantles, but one that reconstructs. In this spirit, the present Section transforms the diagnostic analysis undertaken in Section 4 into a forward-looking framework of remedial action. Rather than merely highlighting deficiencies, it seeks to articulate precise, actionable, and legally coherent interventions that would enable the AI Act to reflect the climate commitments enshrined in the Union's broader legal and policy architecture. Importantly, all recommendations are crafted with the current EU acquis and institutional structure in mind – ensuring that they are not only normatively desirable, but also technically implementable within the bounds of the existing regulatory and procedural ecosystem.

5.1 INCORPORATING CLIMATE RISK INTO HIGH-RISK CLASSIFICATIONS (ANNEX III)

The first and most immediate reform should target Annex III of the AI Act, which exhaustively

[51] Tessel van Oirsouw, 'AI, Digital Sovereignty, and the EU's Path Forward: A Case for Mission-Oriented Industrial Policy' (*Ash Center*, 20 November 2024) <https://ash.harvard.edu/resources/ai-digital-sovereignty-and-the-eus-path-forward-a-case-for-mission-oriented-industrial-policy/> accessed 1 September 2025.

defines 'high-risk' AI applications. A legislative amendment should introduce an additional risk category explicitly dedicated to climate harm. This could include criteria such as:

- High computational energy intensity (e.g., systems consuming over a set megawatt-hour threshold per year);
- Life-cycle carbon emissions above sectoral benchmarks;
- Significant reliance on rare or ecologically harmful materials;
- Water consumption in data training/deployment phases.

These metrics can be benchmarked against the EU Taxonomy Regulation and incorporated into risk classification guidelines issued by the European Commission. Additionally, delegated acts under Article 7 could be used to periodically update climate risk categories as scientific understanding and technical capacity evolve.

A promising avenue for integrating climate risk into the AI Act's high-risk classification scheme lies in drawing on the regulatory methodologies already developed in German public policy. Germany has long incorporated climate impact criteria into sectoral governance frameworks – particularly in energy, infrastructure, and finance – in ways that could inform a more climate-wise robust approach to AI regulation. For instance, under the Bundesverkehrswegeplan 2030 (Federal Transport Infrastructure Plan), German authorities apply a structured climate-related scoring system that assesses projects on the basis of CO^2 emissions, biodiversity effects, and ecosystem fragmentation. Similarly, the Erneuerbare-Energien-Gesetz (Renewable Energy Sources Act, EEG 2021)[52] establishes a long-term objective of achieving greenhouse-gas neutrality for electricity generated and consumed in Germany before 2050. To realise this ambition, the it sets out policy goals and support mechanisms, including remuneration schemes, competitive tenders, and priority access to the grid, thereby defining clear expansion pathways for renewable energy. A further innovation concerns green hydrogen: its production may be fully exempted from the EEG surcharge, or hydrogen producers may benefit from the special equalisation scheme – thus embedding a central element of Germany's national hydrogen strategy within the renewable energy framework and reflecting a broader commitment to integrating climate metrics into ex ante policy planning. At the EU level – where Germany has played an active role – the EU Taxonomy Regulation provides an analogous framework for classifying economic activities based on their climate contributions and compliance with technical sustainability criteria; for instance, under Article 10(1)(a), an economic activity qualifies as contributing substantially to climate change mitigation where that activity contributes substantially to the stabilisation of greenhouse gas concentrations in the atmosphere at a level which prevents dangerous anthropogenic interference with the climate system consistent with the long-term temperature goal of the Paris Agreement through the avoidance or reduction of greenhouse gas emissions or

[52] Bundesministerium für Wirtschaft und Klimaschutz, 'Gesetz zur Änderung des EEG und weiterer energierechtlicher Vorschriften' (*BMWK*, 1 January 2021) <https://www.bmwk.de/Redaktion/DE/Artikel/Service/gesetz-zur-aenderung-des-eeg-und-weiterer-energierechtlicher-vorschriften.html> accessed 1 September 2025.

the increase of greenhouse gas removals, including through generating, transmitting, storing, distributing or using renewable energy. These examples illustrate a best-practice orientation in German regulatory design: one that recognises climate risks as integral to systemic governance. Applying a comparable logic to AI – particularly for resource-intensive or high-emission systems – would not require conceptual innovation, but regulatory transposition. It offers a tested and technically feasible route toward embedding climate risk in the AI Act's foundational structure.

5.2 INTEGRATING CARBON EMISSIONS INTO TECHNICAL DOCUMENTATION (ANNEX IV)

Annex IV should be amended to require climate-linked disclosure within the technical documentation obligations for high-risk AI systems. This may include:

- Disclosure of lifecycle carbon and water footprints (including hardware manufacture, model training, and deployment);
- Energy efficiency benchmarks for inference and training;
- Climate trade-offs for proposed model architectures;

These requirements could be operationalised through implementing acts, aligning Annex IV requirements with the Ecodesign for Sustainable Products Regulation and Corporate Sustainability Reporting Directive. Furthermore, such documentation could be made publicly available in part (e.g. via a registry), enhancing transparency and market-driven sustainability. A compelling example[53] of actionable climate-informed governance in the digital sector is offered by TCO Certified, an internationally recognized sustainability certification for IT products. While voluntary, the scheme has gained broad adoption and mandates comprehensive disclosure and third-party verification of key metrics, including energy consumption and carbon emissions. Notably, TCO Certified applies to product categories such as servers, laptops, and displays – core hardware in AI infrastructure – and sets clear benchmarks for energy efficiency and resource stewardship. Its structured approach demonstrates that it is not only technically feasible but also market-compatible to require climate transparency in digital systems. As such, TCO Certified offers a valuable precedent for extending similar obligations under Annex IV of the AI Act, where climate disclosures could be standardized and integrated through implementing acts and interlinked with broader EU climate legislation.

5.3 EMBEDDING CLIMATE METRICS INTO CONFORMITY ASSESSMENT PROCEDURES

Climate compliance should be formally integrated into the conformity assessment architecture of the AI Act. This could be achieved by:

[53] TCO Development, 'TCO Certified, Generation 9 for Notebooks: Edition 2' (TCO Development, 2022) <https://tcocertified.com/files/certification/tco-certified-generation-9-for-notebooks-edition-2.pdf> accessed 1 September 2025.

- Mandating third-party assessors to verify climate performance using harmonised standards;
- Aligning conformity assessment modules with standards developed by CEN/CENELEC that include emissions, energy, and material intensity thresholds;
- Requiring AI system developers to demonstrate alignment with climate objectives defined in the Taxonomy Regulation.

Such reforms would ensure that AI systems not only meet social and safety standards but also advance the EU's climate objectives in a measurable and verifiable manner. A promising example of how artificial intelligence can be harnessed to support measurable climate compliance comes from the UK-based climate tech firm CarbonBright.[54] Leveraging AI, CarbonBright's platform enables real-time assessments of the carbon footprints of consumer goods across their entire lifecycle – from production through to end-of-life recycling. This model illustrates the potential of AI systems not merely as sources of climate impact, but as instruments for lifecycle impact transparency and sustainable product governance. In doing so, it provides a compelling blueprint for how AI-based tools could be integrated into conformity assessment frameworks under instruments such as the EU AI Act, particularly if climate criteria – currently absent – were formally embedded in technical documentation or verification processes. The CarbonBright case therefore underscores the feasibility and added value of mandating lifecycle-based climate metrics in AI system evaluation.

5.4 CLIMATE CONDITIONS FOR ACCESS TO REGULATORY SANDBOXES

Regulatory sandboxes should be restructured to prioritise and reward climate-conscious innovation. Specifically:

- Sandbox admission criteria should include climate merit—preference should be given to AI systems that demonstrate measurable contributions to emissions reductions, circularity, or energy efficiency.
- Climate impact assessment templates should be developed as a condition for entry.
- National authorities should be empowered to monitor and report on the climate outcomes of sandboxed projects.

These changes can be implemented via delegated acts or national-level sandbox guidance, supported by the European AI Office and in coordination with the EEA (European Environment Agency).

An instructive example of operationalising climate-related principles within AI governance comes from Australia's Commonwealth Scientific and Industrial Research Organisation

[54] CarbonBright, 'Using AI for Sustainability: Case Studies and Examples' (Coaxsoft, 2024) <https://coaxsoft.com/blog/using-ai-for-sustainability-case-studies-and-examples> accessed 1 September 2025.

(CSIRO), which has developed a dedicated ESG-AI Framework.[55] This tool is designed to assist investors, developers, and policymakers in evaluating the climate, resource efficiency, environmental, social, and governance dimensions of AI systems throughout their lifecycle. Unlike general ESG frameworks, CSIRO's model is tailored to the specificities of AI, addressing both systemic risks and sector-specific challenges such as algorithmic opacity, energy consumption, and social externalities. It enables stakeholders to assess AI technologies not only for compliance, but also for their alignment with long-term climate outcomes. By offering practical indicators and guidance for due diligence, the framework represents a leading model for how climate-aligned assessment protocols can be embedded into AI innovation ecosystems – including regulatory sandboxes. Its structure is particularly relevant for jurisdictions like the EU, where proposals have been made to align conformity assessments and sandbox eligibility criteria with the Union's climate objectives, such as the one proposed by Google in March 2025 in the Policy Roadmap 'The AI Opportunity for Europe's Climate Goals'.[56]

5.5 INSTITUTIONALISING NET-ZERO AI BY DESIGN

Under the current version of the AI Act, the climate-aligned development of artificial intelligence remains largely marginalised. To remedy this omission, a dedicated provision introducing a 'climate-compatibility by design' obligation could be envisaged, modelled on analogous frameworks found in the Ecodesign for Sustainable Products Regulation**.** Such a provision would require, inter alia:

- the inclusion of an Climate Impact Assessment (CIA) as part of the AI system's risk management file;
- an obligation to evaluate alternative system designs with a view to climate optimisation; and
- the documentation of energy-saving techniques, such as model pruning, quantisation, or the use of low-power training infrastructure.

These obligations could also be operationalised through voluntary codes of conduct under Article 95, which should be reconfigured as co-regulatory instruments within the framework of soft law governance. The European AI Office, in coordination with the Joint Research Centre and other relevant scientific bodies, could take the lead in developing sector-specific design guidelines to ensure that climate considerations are integrated throughout the AI system lifecycle in a technically robust and legally coherent manner.

A particularly illustrative example of climate-conscious AI by design is CodeCarbon,

[55] CSIRO, 'Responsible AI and ESG: Aligning AI Use with Environmental, Social and Governance Objectives' (Commonwealth Scientific and Industrial Research Organisation 2023) <https://www.csiro.au/-/media/D61/Responsible-AI/Alphinity/Responsible-AI-and-ESG.pdf> accessed 1 September 2025.
[56] Google, 'The AI Opportunity for Europe's Climate Goals – A Policy Roadmap' (March 2025) <https://static.googleusercontent.com/media/publicpolicy.google/en//resources/europe_ai_opportunity_climate_action_en.pdf> accessed 1 September 2025.

an open-source Python package developed by Mila (Quebec AI Institute), BCG GAMMA, Haverford College, and Comet.ml.[57] The tool integrates directly into machine learning workflows to monitor the energy consumption of CPUs, GPUs, and RAM during training and inference. It then cross-references this data with the carbon intensity of the local electricity grid and the geographical location of the computing resources, translating raw energy use into an estimated quantity of CO^2 emissions. Results are logged in real time and can be exported to collaborative dashboards, making the environmental footprint of different models transparent across research teams. Beyond measurement, CodeCarbon functions as a behavioural nudge: by revealing the hidden climate cost of architectural choices, hyperparameter tuning, or deployment schedules, it encourages developers to shift workloads to cleaner energy grids, adopt more efficient hardware, or streamline models. Early use cases suggest that such adjustments can reduce training-related emissions by up to a third, without compromising model accuracy. In this way, CodeCarbon embeds climate accountability into the development process itself, demonstrating how open-source tools can align AI innovation with decarbonisation objectives.

In brief, the preceding suggestions illustrate that bridging the AI Act's climate lacunae does not require legislative reinvention, but targeted recalibration through existing legal instruments, regulatory procedures, and policy frameworks. By harnessing delegated and implementing acts, aligning with parallel EU legislation such as the Taxonomy Regulation and Ecodesign Regulation, and learning from sectoral best practices, the Union can meaningfully embed sustainability within the AI governance ecosystem. The recommendations offered are not aspirational abstractions – they are technically actionable, procedurally compatible, and normatively aligned with the Union's climate and digital objectives. If enacted, they would mark a decisive step toward restoring coherence between the EU's regulatory ambitions and the climate realities of AI development. In this light, climate neutrality must no longer be a collateral consideration in AI governance, but a structural imperative woven into its legal and operational core.

6 CONCLUSION

All things considered, the EU AI Act inaugurates a new era in global digital regulation by establishing a comprehensive, risk-based legal framework for the governance of AI technologies. Yet, for all its normative ambition and institutional innovation, it reveals a profound asymmetry at the heart of the Union's regulatory paradigm: the structural exclusion of climate consciousness from the governance of artificial intelligence. In its current formulation, the AI Act enshrines a model of technological oversight that is procedurally sophisticated yet silent on climate considerations– prioritising data protection, transparency and human safety, while rendering the climate costs of AI systems invisible to law.

This regulatory silence is striking given the growing evidence of the carbon footprint of AI infrastructures: from the energy-intensive training of foundation models, to the lifecycle

[57] CodeCarbon, CodeCarbon: Track and Reduce CO_2 Emissions from Machine Learning Workloads (GitHub, 2023), accessible at: https://github.com/mlco2/codecarbon, (accessed 25 October 2025).

emissions of data centres, the extraction of rare earth minerals for AI hardware and the carbon intensity of global computational supply chains. Yet none of these dimensions are captured within the Act's core instruments. High-emission AI systems are not classified as high-risk under Annex III. CE conformity assessments include no AI lifecycle GHG emissions or energy-efficiency criteria. Regulatory sandboxes remain unconditioned by climate filters. Post-market monitoring regimes lack any obligation to report or mitigate climate damages, and the broader ecosystem of AI governance remains disconnected from parallel instruments in EU acts, including the EU Taxonomy Regulation, the Sustainable Products Initiative, the European Climate Law and the CSRD.

The implications of this omission are both legal and systemic. First, it compromises the Union's constitutional obligation under Article 191(1) TFEU, final indent to promote measures aimed at combating climate change. Second, it introduces incoherence into the architecture of EU governance, whereby digital innovation is actively regulated while its climate consequences are treated as externalities beyond the purview of binding law. Third, it weakens the operational capacity of the Union to realise the objectives of the European Green Deal, which commits the EU to climate neutrality by 2050 and explicitly positions digitalisation as a lever – not a liability – for green transformation. And fourth, it undermines the credibility of the Union's geopolitical identity as a normative green power capable of exporting sustainability-oriented regulatory models to the global digital economy ('EU as a standard-setter').

This failure is emblematic of a deeper structural flaw in the Union's twin transition strategy. While the digital and green transitions are rhetorically intertwined, they remain institutionally decoupled in practice. Digital legislation continues to evolve around paradigms of data sovereignty, rights-based protection and economic coordination, with no embedded climate logic. Conversely, the climate acquis, though increasingly ambitious, remains technologically agnostic – failing to account for the enabling role and material impacts of AI, cloud computing and algorithmic infrastructures. This bifurcation sustains a model of siloed governance unfit for the complexity of the climate crisis or the realities of hyperconnected technological systems.

Rectifying this asymmetry requires more than marginal amendments or voluntary net-zero pledges. It necessitates a recalibration of regulatory methodology – one that embeds climate responsibility as a constitutive, not ancillary, element of digital law. High-emission AI systems must be reclassified as high-risk. Lifecycle climate impact assessments must become mandatory components of conformity procedures. Regulatory sandboxes must incorporate binding climate filters. A horizontal integration mechanism must be established to ensure alignment between the AI Act and instruments like the EU Taxonomy Regulation, CSRD, Ecodesign Regulation and the Green Deal Industrial Plan.

In the Anthropocene, the legitimacy of technological governance depends on its ability to reconcile innovation with climate viability. If the EU is to lead by example, it must build a regulatory regime for artificial intelligence that is not only rights-based and risk-informed, but also climate-literate and sustainability-anchored. The AI Act, in its present form, falls short of that standard. But it need not remain static. The path forward lies in legislative reimagination – where digital progress and climate stewardship are not competing agendas, but

co-constitutive pillars of a resilient and just European legal order.

Nevertheless, the horizon is not closed. The architecture of European law is not immutable – it evolves through vision, consensus and democratic resolve. If institutions, lawmakers, civil society and industry converge around a shared commitment to driving decarbonisation, the AI Act can be transformed into a vanguard of climate responsibility. The tools exist, the mandate is clear and the moment is ripe. With unity of purpose and clarity of ambition, the European Union still has the power to lead a digital transition that not only empowers humanity, but safeguards the planet that sustains it.

LIST OF REFERENCES

Aseeva A, 'Liable and Sustainable by Design: A Toolbox for a Regulatory Compliant and Sustainable Tech' (2024) 16(1) Sustainability 228
DOI: https://doi.org/10.3390/su16010228

Carvão P et al, 'Governance at a Crossroads: EU AI Regulation and Environmental Policy' (M-RCBG Associate Working Paper Series No. 251, Harvard Kennedy School, 2024) <https://www.hks.harvard.edu/sites/default/files/Final_AWP_251_2.pdf> accessed 1 September 2025

Ebert K et al, 'AI, Climate, and Regulation: From Data Centers to the AI Act' (*SSRN*, 22 November 2024) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4980340> accessed 1 September 2025
DOI: https://doi.org/10.2139/ssrn.4980340

'NOT PROHIBITIVELY EXPENSIVE' UNDER THE AARHUS CONVENTION ARTICLE 9(4)

VETLE MAGNE SEIERSTAD*

This article explores the obligation of State Parties to the Aarhus Convention, under Article 9(4), to ensure that costs for accessing justice are 'not prohibitively expensive'. The analysis reveals that this criterion has two sides. Firstly, the level of costs must not be excessive, both in relation to the dispute and object at hand and in relation to the financial resources and what is at stake for a complainant. Secondly, the rules and framework for imposing legal costs must not be unforeseeable. The threshold for costs being prohibitive is when the costs are so excessive or unforeseeable that they will be dissuasive for environmental defenders seeking access to justice. In practice, problems have particularly arisen in regard to 'loser pays' systems, which combine high potential costs with low foreseeability. Such systems are permissible but should have limits on the level of imposable costs and on the judicial discretion that can be exercised.

1 INTRODUCTION

Access to justice is a central and necessary feature of the modern *rechtsstaat*. For human rights to be upheld, and for the judicial branch of government to act as an effective check on the legislative and executive branch, there must be broad and effective access to justice. This is recognised in most modern human rights instruments,[1] and is a reflection of the role of the judiciary in a modern doctrine of separation of powers. The judiciary is firstly a tool to ensure and check that laws are upheld and applied, and secondly, often plays a counter-majoritarian role in protecting interests that struggle to win majoritarian support in a democracy – typically individuals or minority groups.

For the environment, and damages to the environment, the role of the judiciary and effective access to justice is even more pressing. The environment has no democratic voice, and the consequences of environmental damage will largely be felt by groups with no democratic voice, including future generations and people in other countries – even though we all rely on our common environment for our ability to survive and thrive.

Furthermore, environmental law grants rights that primarily protect the environment itself, as a public interest or common good available to all. This makes it different from many

* Legal adviser at the Norwegian Human Rights Institution (NIM) in Oslo, Norway. This article is derivative of broader work done at NIM on the Aarhus Convention. Thanks to colleagues, in particular Hannah Cecilie Brænden, for collaboration in developing and setting out these arguments and for feedback and proofreading.

[1] European Convention on Human Rights (adopted 4 November 1950, entered into force 3 September 1953), 213 UNTS 221 (ECHR), Articles 6 and 13; International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR), Articles 2(3) and 14; American Convention on Human Rights (adopted 22 November 1969, entered into force 18 July 1978) 1144 UNTS 123 (ACHR), Article 8 and 25; African Charter on Human and People's Rights (adopted 27 June 1981, entered into force 21 October 1986) 1520 UNTS 217 (Banjul Charter), Article 7; Charter of Fundamental Rights of the European Union [2012] OJ C326/391 (EU Charter, CFR), Article 47.

other sectors of law where individuals or groups have clear economic or personal incentives to seek access to justice to uphold their own rights. The direct beneficiary of many environmental rules – the environment itself – cannot access justice, and individuals or groups have fewer personal incentives to uphold collective or public environmental interests. This makes it particularly important to remove barriers to accessing effective justice in environmental matters. Otherwise, there is a risk that environmental rules exist solely on paper, with few having the incentives, means and possibilities of upholding them.

This is the problem that Article 9(4) of the Aarhus Convention[2] seeks to rectify. In order to protect the right set out in Article 1 of the Convention, to a healthy, clean and sustainable environment, the Aarhus Convention sets out its pillar of ensuring access to justice in Article 9. Article 9(4) specifically tries to solve the cost- and incentive-barriers to accessing justice, by requiring that procedures be 'not prohibitively expensive'.

This article will answer the question of when, exactly, costs are 'prohibitively expensive'. To do so, Section 2 will first cover some general points on interpreting the Aarhus Convention. Section 3 will then thoroughly analyse the 'not prohibitively expensive'-requirement. Section 3.1 takes a closer look at the text, context and purpose of Article 9(4), finding that costs can be 'prohibitively expensive' both where the level is excessive and where the rules lack foreseeability. Sections 3.2 and 3.3 build on that by diving deeper into when costs are, respectively, prohibitive on account of the level of costs and on account of lacking foreseeability, based on the practice of the Aarhus Committee and the CJEU.

The article adds to the growing literature and use of the Aarhus Convention. Article 9(4) has seen consistent and increasing use both by academics and by legal practitioners, including by NHRIs.[3] That said, most literature on the 'not prohibitively expensive'-requirement has analysed specific cases,[4] or commented on it as part of a broader point on access to justice.[5] This article expands on that literature by more comprehensively analysing when costs are 'prohibitively expensive', in light of the now extensive practice of both the Aarhus Committee and CJEU.

---

[2] Convention on Access to Information, Public Participation in Decision-Making and Access to Justice in Environmental Matters (adopted 25 June 1998, entered into force 30 October 2001), 2161 UNTS 447 (Aarhus Convention).

[3] See for example the reports of the Swedish Institute for Human Rights and of the Norwegian Human Rights institution (from which this article derives) to the 2025 reporting cycle of the Aarhus Convention, commenting on how Article 9(4) has been implemented in Sweden and Norway respectively. Both reports are available here <https://unece.org/environmental-policy/public-participation/2025-reporting-cycle/organisations> accessed 4 October 2025.

[4] See for example; Gayatri Sarathy, 'Costs in Environmental Litigation: Venn v Secretary of the State for Communities and Local Government' (2015) 27(2) Journal of Environmental Law 313; Geert De Baere and Janek Tomasz Nowak, 'The right to not prohibitively expensive judicial proceedings under the Aarhus Convention and the ECJ as an international (environmental) law court: *Edwards and Pallikaropoulos*' (2016) 53(6) Common Market Law Review 1727; Christoph Sobotta, 'New Cases on Article 9 of the Aarhus Convention' (2018) 15(2) Journal of European Environmental & Planning Law 241.

[5] See for example: Vasiliki Karageorgou, 'Access to Justice in Environmental Matters: The Current Situation in the Light of the Recent Developments at the International and Regional Level and the Implications at the National Level with Emphasis on the UNECE Region and the EU MS' (2018) 27(6) European Environmental Law Review 251; Jerzy Jendrośka, 'Access to Justice in the Aarhus Convention – Genesis, Legislative History and Overview of the Main Interpretation Dilemmas' (2020) 17(4) Journal of European Environmental & Planning Law 372.

2 INTERPRETING THE AARHUS CONVENTION

As a treaty, the Aarhus Convention must be interpreted in line with standard methodology as expressed in the Vienna Convention on the Law of Treaties,[6] according to which a treaty shall be interpreted according to its 'ordinary meaning […] in their context and in the light of its object and purpose', see Article 31(1).

When interpreting the Aarhus Convention, account must therefore be taken of the specific context of that Convention, and its object and purpose. In that regard, the Convention sets out its own – and a very broad – purpose in Article 1, to 'contribute to the protection of the right of every person of present and future generations to live in an environment adequate to his or her health and wellbeing'.

This is a recognition of the existence of a right – including for future generations – to a clean, healthy and sustainable environment.[7] This general purpose and right is operationalised through the three different pillars of the Aarhus Convention: (i) the right to environmental information; (ii) the right to participation; and (iii) the right to effective remedies and access to justice. These pillars, and thus the specific provisions and rights enshrined in the treaty, must be interpreted in light of the broader right and purpose in Article 1.[8] This general purpose can lead to a dynamic interpretation where the rights of the Convention can evolve, in the sense that the interpretation of the three pillars might change over time depending on what is necessary to best uphold the right to a clean, healthy and sustainable environment.[9]

Article 15 of the Aarhus Convention, as implemented by the Meeting of the Parties, established the Aarhus Convention Compliance Committee (the Aarhus Committee) for 'reviewing compliance with the provisions of this Convention'. In pursuit of this task, it was given competence to review individual complaints.[10]As the expert body established by the Parties to monitor compliance, its decisions are not legally binding but can still give important guidance on the interpretation of the Convention.[11] Furthermore, where the Aarhus

---

[6] Vienna Convention on the Law of Treaties (adopted 23 May 1969, entered into force 27 January 1980), 1155 UNTS 331 (Vienna Convention).

[7] Also confirmed in recital 7.

[8] As confirmed in recital 8. Cf. for a similar interpretation of provisions in light of a general provisions setting out an objective: *Obligations of States in Respect of Climate Change*, ICJ Advisory Opinion of 23 July 2025, General List No. 187, paras 197, 225 and 231.

[9] See for such an argument: Emily Barritt, 'The Aarhus Convention and the Latent Right to a Healthy Environment' (2024) 36(1) Journal of Environmental Law 67, 74. Such a view has also been advocated by the Aarhus Committee, stating that 'concomitant implementation of the rights under the Convention, in general, should be strengthened over time', see *Communication ACCC/C/2011/57, Denmark,* ECE/MP.PP/C.1/2012/7 para 46.

[10] Article 15 obliges the Meeting of the Parties to adopt a review mechanism, and this was done in Decision I/7, *Review of Compliance*, ECE/MP.PP/2/Add.8 which established the Aarhus Committee, with the annex setting out its structure and the functions.

[11] See the Opinion of AG Kokott in Case C-43/21 *FCC Česká republika* EU:C:2022:425 point 45: 'The decision-making practice of the Aarhus Convention Compliance Committee […] provides important guidance on the interpretation of that provision'. Cf. also the statements of the ICJ on the Human Rights Committee, where 'it believes that it should ascribe great weight to the interpretation adopted by this independent body that was established specifically to supervise the application of that treaty', see *Ahmadou Sadio Diallo (Republic of Guinea v. Democratic Republic of the Congo)*, Merits, Judgment, I.C.J. Report 2010, p. 369, para 66. However, as the ICJ clarified in *Application of the International Convention on the Elimination of All Forms of Racial Discrimination (Qatar v. United Arab Emirates)*, Preliminary Objections, Judgement, ICJ Reports 2021, p. 71, in regards to the CERD Committee, it will not follow the pronouncements of such bodies where

Convention Meeting of the Parties has endorsed or made decisions in accordance with the views of the Committee, this could be considered subsequent agreements or practice under the Vienna Convention, which shall always be taken into account.[12]

Finally, the EU is a party to the Convention and has adopted legislation implementing it, including specifically the obligation to ensure that costs are 'not prohibitively expensive'.[13] This means that there is extensive case-law from the Court of Justice of the European Union (CJEU) which directly and/or indirectly interprets the Aarhus Convention. While that court does not as such have any authoritative role in interpreting the Convention, it could be considered a supplementary means of interpretation.[14] Despite these limitations, CJEU case-law is practically important due to the lack of other decisions or authoritative interpretations of the Aarhus Convention, and because the EU and its Member States make up over half of the State Parties.

3 WHEN ARE COSTS 'PROHIBITIVELY EXPENSIVE'?

3.1 COSTS ARE PROHIBITIVE IF THEY DISSUADE APPLICANTS

Article 9(4) has the following wording (emphasis added):

> In addition and without prejudice to paragraph 1 above, the procedures referred to in paragraphs 1, 2 and 3 above shall provide adequate and effective remedies, including injunctive relief as appropriate, and be fair, equitable, timely and *not prohibitively expensive*. Decisions under this article shall be given or recorded in writing. Decisions of courts, and whenever possible of other bodies, shall be publicly accessible.

For State Parties, this imposes an obligation of result ('not prohibitively expensive') and not one of conduct. States will likely have a large margin to decide how to ensure that costs are

applying 'the relevant customary rules on treaty interpretation' leads to a different conclusion, see para 101. Under the Vienna Convention (n 6), the Committee decisions would likely be considered a 'supplementary means of interpretation' under Article 32.

[12] See the Vienna Convention (n 6) Article 31(3)(a) and (b). Compare the statements of the ICJ on the decisions of similar governing bodies under the climate change treaty framework in *Obligations of States in Respect of Climate Change*, ICJ Advisory Opinion of 23 July 2025, General List No. 187 para 184.

[13] See Directive 2010/75/EU of the European Parliament and of the Council of 24 November 2010 on industrial emissions (integrated pollution prevention and control) [2010] OJ L334/17 Article 25(4); Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on the assessment of the effects of certain public and private projects on the environment (codification) [2012] OJ L26/1 Article 11(4); Directive (EU) 2024/1760 of the European Parliament and of the Council of 13 June 2024 on corporate sustainability due diligence and amending Directive (EU) 2019/1937 and Regulation (EU) 2023/2859 [2024] OJ L2024/1760 Article 29(3)(b) and recital 82; Directive (EU) 2024/2881 of the European Parliament and of the Council of 23 October 2024 on ambient air quality and cleaner air for Europe [2024] OJ L2024/2881 Article 27(2); Directive (EU) 2024/3019 of the European Parliament and of the Council of 27 November 2024 concerning urban wastewater treatment [2024] OJ L2024/3019 Article 25(1).

[14] See the Vienna Convention (n 6) Article 32 on 'supplementary means of interpretation'. Cf. also the Statute of the International Court of Justice (24 October 1945), XV UNCIO 355, article 38(1)(d), on 'judicial decisions' as a 'subsidiary means for the determination of rules of law'.

not prohibitively expensive, but a more limited margin for deciding when that threshold is reached.[15]

The wording of Article 9(4) does not make it clear what is meant by, or when costs are, 'prohibitively expensive'. The use of 'prohibitive' implies a focus, not on the costs themselves, but on the consequences of the costs for the relevant parties. In other words, whether the costs prevent (prohibit) relevant parties (environmental defenders) from having access to justice. This is even clearer in the French wording, which omits the word 'expensive' and just says *'sans que leur coût soit prohibitif'*. The wording itself therefore supports a reading where the central question concerns the consequences of the costs – a consequence-oriented analysis.

The requirement that costs be not prohibitively expensive in Article 9(4) is set out in the context of a broader obligation to 'provide adequate and effective remedies'. When read in combination, costs would likely be considered prohibitive where access to justice is no longer an effective remedy for environmental defenders.

The wording of Article 9(4) must also be read in light of its purpose in achieving the right enshrined in Article 1. The environment cannot, by itself, claim rights or have access to justice. It relies on individuals or NGOs to advocate on its behalf in the interests of the broader public.[16] As acknowledged by the CJEU in several cases, individuals or NGOs act in the public interest when seeking to uphold environmental rules.[17] Read in light of this purpose, the 'not prohibitively expensive' rule recognises that environmental cases differ from other cases where applicants act in their own interest.[18] Individuals and NGOs that act in the public interest should not be dissuaded to seek access to justice by an excessive personal economic risk.

Taken together, both the wording and objective support a broad reading of Article 9(4) where it is focused on the dissuasive effect (the chilling effect) of high costs if they render access to justice an ineffective remedy for ensuring that environmental rules are upheld. This supports a reading of 'prohibitively' as referring to all the ways in which legal costs, and the framework for imposing costs, can have a dissuasive effect on upholding environmental rules

---

[15] See for such a viewpoint, United Nations Economic Commission for Europe, 'The Aarhus Convention – An Implementation Guide, second edition' (2014) 204. This guide can likely be taken as supplementary means of interpretation under the Vienna Convention (n 6) Article 32. The CJEU has clarified that it is an 'explanatory document, capable of being taken into consideration', but noting that 'the observations in the guide have no binding force and do not have the normative effect of the provisions of the Aarhus Convention', see Case C-279/12 *Fish Legal and Shirley* EU:C:2013:853 para 38.

[16] See similarly by AG Kokott in her Opinion in Case C-260/11 *Edwards and Pallikaropoulos* EU:C:2012:645 point 41: 'the environment cannot defend itself before a court, but needs to be represented, for example by active citizens or non-governmental organisations'. See also the recognition of the right of organisations and the public in the Convention, recital 8 and 18, and Article 2(5).

[17] See Case C-873/19 *Deutsche Umwelthilfe (Réception des véhicules à moteur)* EU:C:2022:857 para 68, stating that 'Imposing those criteria must not deprive environmental associations in particular of the possibility of verifying that the rules of EU environmental law are being complied with, given also that such rules are usually in the public interest, rather than simply in the interests of certain individuals, and that the objective of those associations is to defend the public interest', and Case C-252/22 *Societatea Civilă Profesională de Avocați Plopeanu & Ionescu* EU:C:2024:13 para 74, stating that 'members of the public and associations are naturally required to play an active role in defending the environment'. See also Case C-752/18 *Deutsche Umwelthilfe* EU:C:2019:1114 para 34.

[18] This has also been emphasised by the Aarhus Committee, see *Communication ACCC/C/2014/111*, *Belgium*, ECE/MP.PP/C.1/2017/20 paras 69 and 75, emphasising the 'contribution made by appeals by NGOs to improving environmental protection and […] implementation' and the 'public interest nature of the environmental claims'.

and therefore negatively affect the right to a clean, healthy and sustainable environment as set out in Article 1.

As for the threshold for costs being prohibitive, the wording can on the one hand indicate a high threshold. On the other hand, the context (assuring an effective remedy) and the broader objective in achieving the right set out in Article 1 speak in favour of a lower threshold. A level of costs which is such as to dissuade individuals or NGOs from upholding public interests and environmental rules in court would be detrimental to achieving the objective in Article 1.

Account must also be had of whether the rules regulating legal costs are prohibitive on account of their lack of foreseeability. Support for such a reading of Article 9(4) can be found by reading it in conjunction with the general obligation in Article 3(1), requiring each party to 'establish and maintain a clear, transparent and consistent framework to implement the provisions of this Convention'.[19] Such an interpretation implies that costs can be prohibitive if the provisions regulating them and their imposition are not 'clear, transparent and consistent'. Essentially, the lack of legal and economic foreseeability could be dissuasive and have a chilling effect for potential applicants, reducing their effective access to justice.

In summary, 'prohibitively expensive' encompasses all the ways in which legal costs can be dissuasive for an environmental defender, including both the level of costs and the foreseeability of the legal framework,[20] in so far as either can have a dissuasive effect – the threshold for which should not be set too high. Costs could likely have dissuasive effects both if they are disproportionate to the dispute, if they are excessive in relation to the resources available to an applicant, and if they are difficult to foresee, both regarding their imposition and the amount imposed.

That interpretation is supported by the practice of the Aarhus Committee and of the CJEU, which both take a comprehensive view of the cost systems of the Party concerned where they consider all the costs arising from the proceedings.[21] In doing so, they consider both the proportionality or excessiveness of the costs[22] and the foreseeability of the costs.[23] The overarching focus seems to be on whether the level of cost is such as to decrease the

---

[19] Such a *systemic* reading is also supported by the practice of the Aarhus Committee, see: Communication *ACCC/C/2008/33, United Kingdom of Great Britain and Northern Ireland*, ECE/MP.PP/C.1/2010/6/Add.3, para 140 and Decision IV/9i, ECE/MP.PP/2011/2/Add.1 of the Meeting of the Parties paras 3(a) and (d); *Communication ACCC/C/2015/130, Italy*, ECE/MP.PP/C.1/2021/22, paras 118–121 and Decision VII/8j, ECE/MP.PP/2021/2/Add.1, of the Meeting of the Parties, paras 1(f) and (g) and 2(e) and (f).

[20] See similarly: De Baere and Nowak (n 4); Eline Sandnes Fosse, 'Er det "prohibitively expensive" å ta miljøsaker til retten? – Om sakskostnadar som hinder for reell tilgang til domstolsprøving av miljøsakar etter Århuskonvensjonen artikkel 9' (2024, Master Thesis, University of Bergen) section 3.

[21] *Communication ACCC/C/2011/57, Denmark,* ECE/MP.PP/C.1/2012/7, para 45; *Communication ACCC/C/2014/111*, *Belgium*, ECE/MP.PP/C.1/2017/20, para 65; Case C-260/11 *Edwards and Pallikaropoulos* EU:C:2013:221 paras 27–28.

[22] *Communication ACCC/C/2012/77, United Kingdom of Great Britain and Northern Ireland*, ECE/MP.PP/C.1/2015/3, paras 72–75; *Communication ACCC/C/2014/111*, *Belgium*, ECE/MP.PP/C.1/2017/20, paras 66–84; Case C-260/11 *Edwards and Pallikaropoulos* EU:C:2013:221 paras 38–48.

[23] *Communication ACCC/C/2008/33, United Kingdom of Great Britain and Northern Ireland*, ECE/MP.PP/C.1/2010/6/Add.3, paras 135 and 140; *Communications ACCC/C/2013/85 and ACCC/C/2013/86, United Kingdom of Great Britain and Northern Ireland*, ECE/MP.PP/C.1/2016/10, paras 108–112; Case C-427/07 *Commission v Ireland* EU:C:2009:457 paras 93–94; Case C-530/11 *Commission v United Kingdom* EU:C:2014:67 para 35.

number of environmental appeals (i.e. whether the costs are dissuasive).[24]

It must be noted that none of these requirements categorically prevent a court from imposing costs. Article 9(4) must here be read in conjunction with article 3(8), which specifies that 'reasonable costs' may be awarded in judicial proceedings.[25]

The following sections will analyse more closely when costs are, and have been found to be, 'prohibitive'. As stated, costs can be prohibitive both in terms of their level and their foreseeability, and these will be considered separately. Section 3.2 will consider when costs are 'prohibitive' on account of their amount or excessiveness and Section 3.3 will consider when costs are 'prohibitive' on the account of being unforeseeable.

3.2 DISSUASION BY AN EXCESSIVE LEVEL OF COSTS

As stated above, one of the clear requirements of Article 9(4) was that costs would be considered prohibitive if they were excessive or unreasonable to a level which could be dissuasive. The practice of both the Aarhus Committee and the CJEU indicates that this requirement has both objective and subjective components,[26] even if neither of them distinguish between them in a clear or consistent manner. Rather, it seems more like the question of whether costs are prohibitive is considered concretely in that specific case, taking account of both objective and subjective elements where relevant.

Objectively, the Convention requires that the level of costs is not dissuasive. In evaluating this, costs cannot be viewed completely in isolation – but have to be considered in relation to the form and object of a dispute. It is clear from the practice of the Committee that even very small costs can be considered objectively 'prohibitive'. In a complaint against Denmark, the Committee found that 3000 DKK (roughly 400 EUR), which was payable as a fee for complaining to an environmental tribunal, was prohibitive.[27] Small costs have also been found to be prohibitive in another case against Italy, regarding a 650 and 975 EUR filing fee for access to administrative courts.[28]

Obviously, not all costs of roughly 400 EUR (or 975 EUR) would be in breach of Article 9(4). The point seems to be that the fee in that complaint was excessive in relation to the form and objective of disputes in such a tribunal, which was precisely meant as a low-cost alternative where environmental rules can be upheld even in smaller disputes. These complaints indicate that analysis of costs must consider the object of dispute, the form

---

[24] Se *Communication ACCC/C/2011/57, Denmark,* ECE/MP.PP/C.1/2012/7, paras 50–52; *Communication ACCC/C/2015/130 concerning compliance by Italy*, ECE/MP.PP/C.1/2021/22, paras 79, 96 and 104, talking about 'deterrent effect'. This, however, cannot be taken to mean that because the specific applicant has *not* been deterred, the costs are therefore *not* of a level dissuasive or prohibitively expensive to applicants more generally, see Case C-260/11 *Edwards and Pallikaropoulos* EU:C:2013:221 paras 43 and 47.

[25] See for such a reading: Case C-470/16 *North East Pylon Pressure Campaign and Sheehy* EU:C:2018:185 para 60; Case C-252/22 *Societatea Civilă Profesională de Avocați Plopeanu & Ionescu* EU:C:2024:13 para 72.

[26] *Communication ACCC/C/2012/77, United Kingdom of Great Britain and Northern Ireland*, ECE/MP.PP/C.1/2015/3, para 72: 'Moreover, such an assessment should involve both objective and subjective elements'; Case C-252/22 *Societatea Civilă Profesională de Avocați Plopeanu & Ionescu* EU:C:2024:13 para 74: '[…] the cost of proceedings must neither exceed the financial resources of the person concerned nor appear, in any event, to be objectively unreasonable'.

[27] See *Communication ACCC/C/2011/57, Denmark,* ECE/MP.PP/C.1/2012/7, paras 43–52.

[28] See *Communication ACCC/C/2015/130, Italy*, ECE/MP.PP/C.1/2021/22, paras 72–80, endorsed by the Meeting of the Parties in Decision VII/8j, ECE/MP.PP/2021/2/Add.1, para 1(a) and (b).

of the proceedings and the type of costs imposed,[29] and that even small costs can be prohibitive if they are not justified by any of these factors.

Such an interpretation is in line with the general wording and purpose of Article 9(4). If 'prohibitively' was interpreted as setting a general norm, level or cap that is prohibitive, applicable to all cases, it would be ineffective for small-scale comparatively cheap proceedings dealing with local environmental issues, which are less costly than say large-scale litigation over constitutional principles. Those small cases, due to their potentially large number, are still very important for ensuring compliance and implementation. Precisely because those cases are rarely matters of principle, even moderate costs can be very dissuasive.

Article 9(4) should therefore be interpreted to require an analysis of whether costs are dissuasive which includes comparing the costs to the form and object of the dispute at hand. For a local or low-complexity dispute, even smaller costs can have a clear dissuasive effect. Such an interpretation ensures that effective access to justice can be ensured for all types of environmental rules and cases.

The relative sense of that conclusion makes it hard to say anything generally on when legal costs will be considered, objectively, of a too high level and therefore prohibitively expensive. It will require a comprehensive consideration of several factors, including the level of income and costs in that country, the costs in the specific case, the form and object of the dispute, and an evaluation of whether costs like that are likely to be – or have been – dissuasive. It will also be relevant to consider how large the public interest in the case is,[30] in line with the broader objective of the Convention in Article 1. For example, a large environmental and public interest could be proven by reference to similar appeals often leading to the repeal of illegal decisions.[31]

The Committee has dealt with some complaints that can give guidance on when costs are likely to be prohibitively expensive. Most complaints deal with costs being imposed on the losing party. In a case against the UK, the Committee considered costs of 8 000 GBP (not inflation adjusted) imposed on the losing party, Greenpeace, as causing the proceedings to be 'prohibitively expensive', despite the Court having lowered the costs compared to the original amount of 11 813 GBP. In arriving at that conclusion, the Committee emphasised the importance of the object of dispute, the importance of the public interests and lack of other avenues to defend them and the costs incurred by Greenpeace for its own lawyers.[32]

---

[29] See also, for such a view, *Communication ACCC/C/2016/142, United Kingdom of Great Britain and Northern Ireland*, ECE/MP.PP/C.1/2021/27, para 101, where the Committee points out that the type and form of procedure being considered is 'a significantly less complex matter than a judicial review procedure in the vast majority of cases' which should 'be an efficient and accessible mechanism'. The less complex and accessible nature of the proceedings was an argument in favour of the costs being prohibitive.

[30] Case C-252/22 *Societatea Civilă Profesională de Avocați Plopeanu & Ionescu* EU:C:2024:13 paras 74–75. This includes being able to consider, to the detriment of an applicant, whether the claims are potentially frivolous. For the latter, see also Case C-470/16 *North East Pylon Pressure Campaign and Sheehy* EU:C:2018:185 paras 59–65.

[31] As the Committee emphasised in *Communication ACCC/C/2011/57, Denmark,* ECE/MP.PP/C.1/2012/7, para 49.

[32] *Communication ACCC/C/2012/77, United Kingdom of Great Britain and Northern Ireland*, ECE/MP.PP/C.1/2015/3, paras 72–77. The conclusion was endorsed by the Meeting of the Parties in Decision VI/8k, ECE/MP.PP/2017/2/Add.1, para 3.

The UK amended its regulatory framework by introducing a system of 'Aarhus claims', with a cap for the imposition of legal costs amounting to 5 000 GBP for individuals and 10 000 GBP for organisations. This was evaluated by the Committee, which was 'not convinced' that this would not be prohibitively expensive, noting that applicants would have to cover their own cost in addition to these.[33] In another complaint, against Italy, the Committee also expressed similar scepticism towards a level of imposed costs ranging from 2 000 EUR to 5 000 EUR imposable per defendant, which could come in addition to other costs or fees.[34] However, in an earlier case, the Committee expressed, in relation to a cost order of 5 130 GBP (not inflation adjusted), that the 'quantum of the order' was not prohibitively expensive by itself.[35]

The cases illustrate that it is difficult to set a clear level where the cost will typically be prohibitive, even on the higher end. All these cases concerned costs imposed on the losing party, and ranges like the ones in these cases will likely create a risk of costs being considered prohibitive in at least some cases, but it has to be analysed specifically and individually in relation to the case at hand.

While most cases deal with costs being imposed on the losing party, the Committee has also dealt with the level of total costs, including what an applicant has to pay for their own lawyers. The Committee found, in a case against the UK, that a general level of costs for 'private nuisance claims' which typically exceeded 100 000 GBP, without any adequate alternative procedures, was prohibitively expensive.[36] This makes clear that a very high level of costs can be prohibitive even in the absence of being held liable for the opponents legal costs, and that high own legal fees are also relevant for considering whether the level of costs is objectively prohibitive.

Subjectively, legal costs can be prohibitively expensive in relation to a specific applicant and their economic situation,[37] in light of the importance of the case for that applicant.

A subjective evaluation can include considering all aspects of the applicant's economic situation. For NGOs, the Committee has mentioned factors like the number of members, the membership fee and the resource allocation of the NGO to judicial activities as compared to other activities.[38] The CJEU has clarified that this can include the importance of what is at stake for the claimant.[39] A subjective evaluation can also likely include the degree to which the applicant is to blame for the costs incurred or not.[40]

---

[33] *Compliance by the United Kingdom of Great Britain and Northern Ireland*, ECE/MP.PP/2014/23, para 47. The Committees general findings were endorsed by the Meeting of the Parties in Decision V/9n, ECE/MP.PP/2014/2/Add.1, para 2.

[34] *Communication ACCC/C/2015/130, Italy*, ECE/MP.PP/C.1/2021/22, paras 89–98. The Committee's conclusion was endorsed by the Meeting of the Parties in Decision VII/8j, ECE/MP.PP/2021/2/Add.1), para 1(c).

[35] *Communication ACCC/C/2008/23, United Kingdom of Great Britain and Northern Ireland*, para 49.

[36] *Communications ACCC/C/2013/85 and ACCC/C/2013/86, United Kingdom of Great Britain and Northern Ireland*, ECE/MP.PP/C.1/2016/10, paras 105–114, endorsed by the Meeting of the Parties in Decision VI/8k, ECE/MP.PP/2017/2/Add.1, para 5, see also the recommendation in para 6.

[37] See above n 26.

[38] *Communication ACCC/C/2011/57, Denmark,* ECE/MP.PP/C.1/2012/7, para 47.

[39] Case C-260/11 *Edwards and Pallikaropoulos* EU:C:2013:221 para 42.

[40] Cf. *Communication ACCC/C/2008/23, United Kingdom of Great Britain and Northern Ireland*, para 52, where the Committee emphasised that the applicants had initiated cheaper methods of resolution, which had been declined.

The fact that the applicant actually has asserted a claim and therefore has not, in practice, been deterred from accessing justice cannot by itself establish that the proceedings are not prohibitively expensive for them.[41]

Given that a subjective evaluation will vary widely from case to case, there is not much guidance from the Committee or the CJEU in terms of amounts. However, in a case against Belgium the Committee did view costs of 3700 EUR (not inflation adjusted) as imposing 'a considerable financial burden on the communicants' and that 'costs of this level could effectively prevent small environmental NGOs from challenging decisions, acts and omissions', but found that the specific applicants had not supplied sufficient evidence as to their economic situation.[42] This at least provides an indication of sums that might typically be prohibitive for smaller applicants.

Some types of cases are naturally more expensive than others, due to the complexity or object of the case. It seems unlikely that the Aarhus Convention would require that the level of costs in the most complex cases not exceed the financial resources of the smallest applicants. The purpose of the Convention in Article 1 can be upheld as long as there is a sufficient group of NGOs or individuals that can act as applicants in all types of cases. The Aarhus Convention also, most likely, does not intend to encourage the formation of smaller NGOs with less economic resources for use in strategic litigation as a means to avoid legal costs. In evaluating how important the case is for the applicant at hand, recourse may therefore likely be had to how the object of the dispute relates to the work of the NGO, its representativeness, members and the reasons for its establishment. For other groups and individuals, account can likely also be had of whether they are directly and individually affected and have a lot at stake, in a way that makes them the most natural representative of the affected interests even if they might lack the resources of larger groups or NGOs.

In total, costs can have a dissuasive effect by being high compared to the form and object of the dispute and by being high compared to the importance for, and resources available to, the applicants.

A last point to note in relation to both categories is that the costs of an applicant are not just affected by their own incurred costs but also by expenses they themselves can seek covered or recovered. In this sense a loser pays system will, in some cases, make costs less dissuasive because a successful applicants can have their costs covered. If State Parties consider systems that cap the liability for costs, a system capping it only one way ('one-way cost-shifting') would be less dissuasive for applicants,[43] whereas a system that caps also the costs that applicants can recover risks making cases 'too expensive to win'.[44]

A one-way cost-shifting system could also involve the state taking the cost for successful applicants. That would be based on a recognition that the successful applicants

---

[41] Case C-260/11 *Edwards and Pallikaropoulos*, EU:C:2013:221 para 47; Case C-530/11 *Commission v United Kingdom* EU:C:2014:67 para 50.

[42] *Communication ACCC/C/2014/111*, *Belgium*, ECE/MP.PP/C.1/2017/20, para 77, more generally paras 78–84.

[43] This is a solution recommended by the EU Commission, 'Notice on access to justice in environmental matters' [2017] OJ C275/1 para 192.

[44] See similarly, Carol Day et al, 'A Pillar of Justice II; The continuing impact of legislative reform on access to justice in England and Wales under the Aarhus Convention' (2023) p. 35 ('there is a clear risk that the reciprocal cap, particularly when set at the level that it is, can make cases too expensive to win') <https://elflaw.org/wp-content/uploads/2023/06/A-Pillar-of-Justice_Report.pdf> accessed 4 October 2025.

contributed to upholding rules that are in the public interest and the broader objective of the Aarhus Convention in Article 1, and therefore that it would be fair for the public to cover costs.

States can also use legal aid as a means to ensure that costs are not so excessive as to be dissuasive.[45] This might, particularly, be suitable to ensure that costs are not excessive subjectively. However, legal aid systems typically only apply to individuals – thus not helping to ensure that the costs for NGOs are not prohibitive.

3.3 DISSUASION BY UNFORSEEABLE COSTS

The lack of foreseeability of imposed costs is at the core of the criticism from both the Committee and the CJEU in several cases. As mentioned above, Article 9(4) of the Convention must be read in conjunction with Article 3(1), requiring the states to establish a 'clear, transparent and consistent' framework for implementing the Convention.

If access to justice and effective remedies are to help attain the objective in Article 1, the rules regulating them must be as clear as possible. In particular, lack of clear rules when it comes to the imposition of costs on the losing party could be very dissuasive for environmental defenders, often not having extensive resources, nor any economic incentive or reward themselves in the complaints and cases they pursue. While environmental defenders can control and ensure foreseeability of their own legal costs, the risk of being held liable for the legal costs of the other party makes it very difficult to plan, budget and evaluate whether it is worth accessing justice in any specific case.

The Committee has extensively considered the UK system for imposing legal costs, which employs a principle of 'loser pays' while also leaving a lot of discretion to the judge in regards to whether and which costs are actually imposed. The Committee found this system to be problematic, pointing to the lack of clarity in the criteria, the lacking consideration of public interest in the environmental issues at hand and the lack of adequate legal aid or protective costs orders.[46] It found that the UK was in violation of Article 9(4), because

> the considerable discretion of the courts of England and Wales in deciding the costs, without any clear legally binding direction from the legislature or judiciary to ensure costs are not prohibitively expensive, leads to considerable uncertainty regarding the costs to be faced where claimants are legitimately pursuing environmental concerns that involve the public interest.[47]

---

[45] This is a proposed solution by the EU Commission, see the Notice on access to justice in environmental matters (n 43) paras 194–195. Cf. also the IACtHR Advisory Opinion AO-32/25 of May 29, 2025, *Climate Emergency and Human Rights*, para 542, requiring states to provide legal assistance where people cannot afford costs, and citing the Escazú Agreement Article 8, which contains a parallel requirement of 'not prohibitively expensive' costs.

[46] Communication *ACCC/C/2008/33, United Kingdom of Great Britain and Northern Ireland*, ECE/MP.PP/C.1/2010/6/Add.3, paras 129–135.

[47] Communication *ACCC/C/2008/33, United Kingdom of Great Britain and Northern Ireland*, ECE/MP.PP/C.1/2010/6/Add.3, para 135, see also 141, endorsed by the Meeting of the Parties in Decision IV/9i, ECE/MP.PP/2011/2/Add.1, para 3(a). The Committee concluded similarly in *Communications ACCC/C/2013/85 and ACCC/C/2013/86, United Kingdom of Great Britain and Northern Ireland*, ECE/MP.PP/C.1/2016/10, paras 108–112, followed up by the recommendations of the Meeting of the Parties in Decision VI/8k, ECE/MP.PP/2017/2/Add.1, para 6.

The Committee has also pointed to the discretion of courts being a problem in a complaint against Italy: 'the wide discretion conferred on the courts when deciding litigation costs leads to a lack of certainty and clarity regarding the costs that claimants will face when exercising their right to access to justice in environmental matters'.[48]

The CJEU has considered similar discretion in both the Irish and British judicial systems, and has stated that:

> [a]lthough it is common ground that the Irish courts may decline to order an unsuccessful party to pay the costs and can, in addition, order expenditure incurred by the unsuccessful party to be borne by the other party, that is merely a discretionary practice on the part of the courts.
> That mere practice which cannot, by definition, be certain, […] cannot be regarded as valid implementation of the obligations […].[49]

In a later case against the UK, the CJEU stated that:

> [i]t is also apparent from the foregoing that that regime laid down by case-law does not ensure the claimant reasonable predictability as regards both whether the costs of the judicial proceedings in which he becomes involved are payable by him and their amount, although such predictability appears particularly necessary because, as the United Kingdom acknowledges, judicial proceedings in the United Kingdom entail high lawyers' fees.[50]

That said, the CJEU has clarified that Article 9(4) does not prevent courts from exercising some discretion in determining costs,[51] nor does it require a detailed determination of costs in national legislation.[52]

One way of ensuring increased foreseeability and control over costs in 'loser pays' systems is by using a cap-system, where liability is capped at certain sums.[53] This presents the obvious problem, discussed in Section 3.2 in relation to the UK cap, that the cap will likely have to be set rather high to account for complex cases, meaning costs near the cap might be prohibitively expensive for less complex cases.

The Committee approved of a 'loser pays' system that solved some of these issues in a case concerning Belgium. The system employed a modified cap (a cap-range), where the losing party was held liable for a flat contribution to the successful party's costs and legal fees, with a basic amount of 1 320 EUR, a minimum amount of 82.50 EUR and a maximum amount of 11 000 EUR (not inflation adjusted). The basic amount was applied in most cases, but the judge had discretion to modify it within the given range on request, taking account of the nature of the case, the importance of the litigation, its complexity, the unreasonable

---

[48] *Communication ACCC/C/2015/130, Italy*, ECE/MP.PP/C.1/2021/22, para 118. The general point of the framework being unclear and untransparent was endorsed by the Meeting of the Parties in Decision VII/8j, ECE/MP.PP/2021/2/Add.1, para 1(f) and the recommendation in para 2(e).
[49] Case C-427/07 *Commission v Ireland* EU:C:2009:457 paras 93–94. Reiterated in Case C-530/11 *Commission v United Kingdom* EU:C:2014:67 para 35.
[50] Case C-530/11 *Commission v United Kingdom* EU:C:2014:67 para 58.
[51] ibid para 54.
[52] Case C-252/22 *Societatea Civilă Profesională de Avocați Plopeanu & Ionescu* EU:C:2024:13 para 81.
[53] The European Commission recommends a cap-system as one way of ensuring predictability and control over costs, see the Notice on access to justice in environmental matters (n 43) para 189.

nature of the situation and the unsuccessful party's financial capacity. The Committee found this system to provide more foreseeability and therefore distinguished it from their previous considerations of the UK system.[54]

In total, therefore, 'prohibitively expensive' in Article 9(4) of the Convention must be interpreted as meaning that the lack of foreseeability in relation to the costs of legal proceedings, including the costs being imposed, and the dissuasive effects caused by that, can be considered prohibitive and thus in breach of the Convention. Based on the practice of the Committee and the CJEU, it is particularly the combination of high legal fees, the use of a 'loser pays' system, and the use of high judicial discretion both as to the imposition of costs and as to their amount, which is liable to be dissuasive and therefore prohibitive. A 'loser pays' system might be more acceptable in terms of foreseeability if the amounts imposable and clear criteria to guide the use of judicial discretion are set out in legislation.

Legal aid or assistance-systems can also be a solution where costs are not foreseeable,[55] but as noted above they typically only cover individuals, and so they might not be a solution for NGOs seeking access to justice.

4 CONCLUSION

Article 9(4) of the Aarhus Convention seeks to ensure that it is possible for individuals, groups and NGOs, acting as environmental defenders, to uphold environmental law and therefore the public interest without incurring costs that make it prohibitive for them.

This article sought to answer exactly when costs are 'prohibitively expensive'. As the analysis has shown, the relevant metric is whether costs are dissuasive for a sufficient number of applicants, undermining the achievement of the overarching objective in Article 1 of an environment adequate to health and wellbeing.

The analysis further demonstrated that states, to prevent such a dissuasive effect from legal costs, must have rules regulating both the level of costs and their foreseeability. Whether the level of costs is too high must be considered on the basis of all the costs incurred in the proceedings, including own costs, opponent's costs, and applicable fees. The level of costs can be dissuasive both objectively, in relation to the form, object and importance of a dispute and how it contributes to upholding public interests, and subjectively, in relation to the financial situation of the applicant and what is at stake for them.

Lacking foreseeability can have a dissuasive effect regardless of the level of costs. This is particularly true for the type of costs most of the cases from the Aarhus Committee and the CJEU deal with, which is the risk of being held liable for the opponents' costs ('loser pays'). While Article 9(4) does not preclude such liability inherently, it does preclude them where it is left entirely to judicial discretion without clear criteria, and where there is no foreseeability as to the level of costs that might be and usually are imposed.

A typical solution to the 'loser pays' systems is to introduce a sort of a cap system. As illustrated by some of the complaints against the UK, a universal cap applicable in all cases might be unsuited because it doesn't take account of the objective and subjective elements required. If the cap is set to a high amount, suitable for the more complex cases, it could be

[54] *Communication ACCC/C/2014/111*, *Belgium*, ECE/MP.PP/C.1/2017/2, paras 66–71.
[55] See above n 45.

prohibitively expensive for smaller cases or certain applicants. A better approach is the use of a cap range, like the Belgian system discussed above,[56] with a basic amount and a range limit, with some judicial discretion as to the imposition. That discretion should be delimited by clear and foreseeable criteria, in line with the objective and subjective elements that determine whether costs are prohibitive. It is important to avoid undue judicial discretion, which could undermine the foreseeability the system seeks to ensure.[57]

In general, State Parties will have a wide discretion and range of possibilities for how to ensure that costs remain non-prohibitive, as long as it sufficiently addresses both the level of costs and foreseeability of their imposition. This can include everything from (and a mix of) a cap system, cap-ranges, the state covering certain costs, legal aid- and assistance systems, use of alternative dispute resolution mechanisms and/or tribunals to lower costs, and many other systems. This article has broadly set out the requirements for such systems and given some indications as to what level of costs and which types of rules risk being prohibitive for applicants.

[56] See Section 3.3.

[57] As recommended by the EU Commission in the Notice on access to justice in environmental matters (n 43) para 193 'a discretion which is too wide may undermine cost predictability'.

LIST OF REFERENCES

Barritt E, 'The Aarhus Convention and the Latent Right to a Healthy Environment' (2024) 36(1) Journal of Environmental Law 67
DOI: https://doi.org/10.1093/jel/eqae003

Day C et al, 'A Pillar of Justice II; The continuing impact of legislative reform on access to justice in England and Wales under the Aarhus Convention' (2023) <https://elflaw.org/wp-content/uploads/2023/06/A-Pillar-of-Justice_Report.pdf> accessed 4 October 2025

De Baere G and Nowak JT, 'The right to not prohibitively expensive judicial proceedings under the Aarhus Convention and the ECJ as an international (environmental) law court: *Edwards and Pallikaropoulos*' (2016) 53(6) Common Market Law Review 1727
DOI: https://doi.org/10.54648/COLA2016148

Fosse ES, 'Er det "prohibitively expensive" å ta miljøsaker til retten? – Om sakskostnadar som hinder for reell tilgang til domstolsprøving av miljøsakar etter Århuskonvensjonen artikkel 9' (Master Thesis, University of Bergen 2024) <https://hdl.handle.net/11250/3145461> accessed 4 October 2025

Jendrośka J, 'Access to Justice in the Aarhus Convention – Genesis, Legislative History and Overview of the Main Interpretation Dilemmas' (2020) 17(4) Journal of European Environmental & Planning Law 372
DOI: https://doi.org/10.1163/18760104-01704003

Karageorgou V, 'Access to Justice in Environmental Matters: The Current Situation in the Light of the Recent Developments at the International and Regional Level and the Implications at the National Level with Emphasis on the UNECE Region and the EU MS' (2018) 27(6) European Environmental Law Review 251
DOI: https://doi.org/10.54648/eelr2018030

Sarathy G, 'Costs in Environmental Litigation: Venn v Secretary of the State for Communities and Local Government' (2015) 27(2) Journal of Environmental law 313
DOI: https://doi.org/10.1093/jel/eqv016

Sobotta C, 'New Cases on Article 9 of the Aarhus Convention' (2018) 15(2) Journal of European Environmental & Planning Law 241
DOI: https://doi.org/10.1163/18760104-01502006

TO HOST OR NOT TO HOST: NARROWING INTERMEDIARY LIABILITY EXEMPTION IN THE DSA

JACOB VAN DE KERKHOF*

Intermediary liability exemption in the Digital Services Act (Regulation 2022/2065, 'DSA') is generally interpreted as being unchanged compared to the e-Commerce Directive (Directive 2000/31). Conditional liability exemption strikes a balance between the interests of hosting providers, people affected by illegal content, and the freedom of expression of the general public. However, hosting providers and their role in society have evolved significantly since the adoption of the e-Commerce Directive. Despite their position as key infrastructure in the public debate and their sophisticated content moderation processes, they enjoy a seemingly widening exemption from liability in CJEU case law. This article argues for a narrower scope of application for intermediary liability exemption for hosting services guided by due diligence obligations and duties of care created in the DSA and sectoral regulation. This can benefit aggrieved parties in holding platforms liable and inspire better moderation of illegal content. A narrower interpretation of the liability exemption can be justified by compliance with requirements on notice-and-takedown mechanisms, a fairer economic burden of moderation, improved moderation capacity, and the geopolitical tensions which strain effective content moderation. The DSA provides clear due diligence obligations in Articles 16 and 23, and sectoral regulation requires diligence regarding specific types of content. These obligations can be used to exclude undiligent or bad faith actors from the liability exemption. This better reflects hosting providers' positions as powerful actors and ensures a liability exemption that does not reward negligent or laissez-faire approaches to content moderation by actors that stand to gain monetarily from structurally hosting illegal content.

1 INTRODUCTION

In February 2025, Instagram users were surprised by a large amount of violent and sexual imagery crowding their 'Reels' page. Meta apologised profusely for displaying illegal content to a large number of users; their automated moderation process had malfunctioned.[1] Platforms frequently boast the success of their content moderation systems, increasingly relying on novel techniques such as large-language models to moderate content.[2] The fallibility of such means, together with a changing political landscape in which platforms align

* PhD Candidate, Utrecht University. The Author is grateful for professors Peter Blok, Janneke Gerards, and Catalina Goanta for their guidance and feedback in writing this contribution.

[1] Dylan Butts, 'Meta says it fixed "error" after Instagram users report a flood of graphic and violent content', (CBNC, 26 February 2025) <https://www.cnbc.com/2025/02/27/meta-apologizes-after-instagram-users-see-graphic-and-violent-content.html> accessed 1 September 2025.

[2] For TikTok: Rozanna Latiff, 'ByteDance's TikTok Cuts Hundreds of Jobs in Shift towards AI Content Moderation' (*Reuters*, 11 October 2024) <https://www.reuters.com/technology/bytedance-cuts-over-700-jobs-malaysia-shift-towards-ai-moderation-sources-say-2024-10-11/> accessed 1 September 2025. For Meta: 'Content Moderation in a New Era for AI and Automation | Oversight Board' (*Oversight Board*, 17 September 2024) <https://www.oversightboard.com/news/content-moderation-in-a-new-era-for-ai-and-automation/> accessed 1 September 2025.

with a political trend that promotes less moderation rather than more,[3] underline the importance of an effective liability framework surrounding the hosting of illegal content. A balanced intermediary liability framework strikes an appropriate balance between the interests of aggrieved parties, internet intermediaries, and the general public.

The primary liability exemptions for hosting illegal content in the European Union are laid down in Articles 4-6 Digital Services Act ('DSA')[4] and were previously found in Articles 12-14 of the e-Commerce Directive ('ECD').[5] Intermediary liability for hosting illegal content constitutes a precarious balance between providing a remedy for parties affected by illegal content, protecting the users' freedom of expression from potential over-enforcement as a result of liability, chilling third-party speech, and stumping online platforms in their economic growth. The ECD's doctrine has been developed in case law over the last 25 years.[6] Academic consensus is that, despite the transition from the ECD to the DSA, intermediary liability exemptions have not changed.[7] The DSA has merely adopted some of the Court of Justice of the European Union's (CJEU) reasoning in its recitals to provide context to the liability exemption.[8] However, the landscape around content moderation and the dissemination of illegal content on the internet has developed significantly since 2000. Online platforms have become places where users can socialise, network, participate in the democratic process, and shop, all at the same time.[9] The legal landscape has similarly evolved: the DSA creates a layer of accountability on top of the existing liability rules laid down in the ECD, encompassing a wide range of due diligence obligations, such as transparency obligations, risk assessments, and engagement with civil

---

[3] Jacob van de Kerkhof, 'Musk, Techbrocracy and Free Speech' in Alberto Alemanno and Jacquelyn Veraldi (eds), *Musk, Power, and the EU: Can EU Law Tackle the Challenges of Unchecked Plutocracy?* (Verfassungsbooks 2025) 91 et seq.

[4] 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) [2022] OJ L277/1.

[5] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) [2000] OJ L178/1; see also Raphaël Gellert and Pieter Wolters, 'The Revision of the European Framework for the Liability and Responsibilities of Hosting Service Providers' (Ministry of Economic Affairs and Climate Policy 2021) 99.

[6] E.g. Joined Cases C-236/08 to C-238/08 *Google France v Louis Vuitton* EU:C:2010:159; Case C-324/09 *L'Oreal v eBay* EU:C:2011:474; Joined Cases C-682/18 and C-683/18 *YouTube/Cyando* EU:C:2021:503; but also in the sphere of the Council of Europe: *Delfi v Estonia* App no 64569/09 (ECtHR, 16 June 2015); *Sanchez v France* App no 45581/15 (ECtHR, 15 May 2023); *Patrascu v Romania* App no 1847/21 (ECtHR, 7 January 2025).

[7] E.g. Folkert Wilman, 'The Digital Services Act (DSA): An Overview' (*SSRN*, 27 December 2022), 2 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4304586> accessed 1 September 2025: 'Moreover, as will be seen below, the DSA includes the rules on liability which were previously contained in that directive'; Aleksandra Kuczerawy, 'The Power of Positive Thinking Special Issues: Intermediary Liability as a Human Rights Issue' (2017) 8(3) Journal of Intellectual Property, Information Technology and Electronic Commerce Law 226, 228: 'After consultation, the Commission concluded that it would maintain the existing intermediary liability regime while implementing a sectorial, problem-driven approach'; Martin Husovec, *Principles of the Digital Services Act* (Oxford University Press 2024) 65: 'To avoid [a death sentence for decentralised speech], the second generation of rules, such as the DSA, does not intend to change the underlying liability for someone else's content'.

[8] Ronan Riordan, 'A Case Study of Judicial-Legislative Interactions via the Lens of the DSA's Host Liability Rules' (2025) 10(1) European Papers – A Journal on Law and Integration 259.

[9] Catalina Goanta, 'The New Social Media: Contracts, Consumers, and Chaos' (2023) 108 Iowa Law Review 118; generally Jose van Dijck, *The Culture of Connectivity: A Critical History of Social Media* (Oxford University Press 2013).

society actors.[10] These obligations follow a layered approach, increasing as the size of the platform increases.[11] Very Large Online Platforms and Very Large Online Search Engines ('VLOPSEs', platforms with a number of monthly active users exceeding 45 million)[12] need to abide by the most intense regime,[13] whereas micro- and small enterprises are excluded from the scope of a number of DSA provisions.[14]

The starting point of this contribution is the observation that the DSA maintains – at least in phrasing – the liability exemptions of the ECD in spite of the evolution that hosting providers underwent in the past 25 years. This raises the question whether changes in content moderation and the expectations raised in the DSA should be better reflected in how the doctrine of intermediary liability exemption is applied. This contribution argues that, although the legal phrasing of liability exemptions has not significantly changed since the ECD, it requires nuancing to (a) reflect platforms' poor compliance with mandatory notice-and-action mechanisms, frustrating a pre-condition for liability exemption; (b) reflect the economic reality in which hosting providers benefit economically from hosting illegal content; (c) reflect platforms' improved technological moderation capacity compared to the early 2000s; (d) provide a clearer incentive for platforms to moderate illegal content in a geopolitical landscape that stimulates less moderation; and (e) the observation that the case law of the European Court of Human Rights regarding freedom of expression on the internet does not stand in the way of this argument. Not only can a narrower scope of liability exemption ensure a fairer distribution of responsibility for hosting illegal content, it also provides more remedies for parties aggrieved by illegal content by excluding bad faith actors, and it may stimulate moderation against illegal content,[15] preventing associated harms. The DSA provides clear guidelines that can guide this interpretation of the hosting liability exemption, predominantly through requirements that can exclude non-diligent hosting providers and through expectations around the level of diligence that could lead to awareness of illegal content.

This argument is laid out along the following structure: Section 2 introduces the current framework for liability exemption for hosting illegal content and explains why the consensus is that the DSA has not changed the doctrine for liability exemption since the ECD; Section 3 provides reasons why the intermediary liability exemption should be interpreted more narrowly than 25 years ago; Section 4 explains instances in the DSA and sectoral regulation that can change how intermediary liability exemption is applied in light of requirements for platform due diligence. The purpose of this article is not to dismiss intermediary liability exemption; it argues for a nuanced narrowing of scope of the liability

[10] Martin Husovec, 'Rising Above Liability: The Digital Services Act as a Blueprint for the Second Generation of Global Internet Rules' (2023) 38 Berkeley Technology Law Journal 883. See also Rachel Griffin, 'Public and Private Power in Social Media Governance: Multistakeholderism, the Rule of Law and Democratic Accountability' (2023) 14(1) Transnational Legal Theory 46.
[11] Digital Services Act (n 4) recital 76; see also Folkert Wilman, 'De Digital Services Act (DSA): een belangrijke stap naar betere regulering van onlinedienstverlening' (2022) 28 Nederlands tijdschrift voor Europees Recht 220, 222.
[12] Digital Services Act (n 4) Article 33(1).
[13] ibid Section 5 Articles 33-43.
[14] As defined in Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises [2003] OJ L124/36; Digital Services Act (n 4) Articles 15(2), 19(1), 29(1).
[15] E.g. Yassine Lefouili and Leonardo Madio, 'The Economics of Platform Liability' (2022) 53 European Journal of Law and Economics 319.

exemption in cases where hosting providers act negligently in their due diligence obligations in content moderation.

2 INTERMEDIARY LIABILITY EXEMPTION IN THE DSA

Before expanding on arguments for narrowing the scope of intermediary liability exemption in Section 3, this section explains the framework for intermediary liability exemption for hosting illegal content in the DSA and why it resembles that of the ECD. Important to note at the outset is that the DSA only harmonises the exemption of liability for hosting illegal content; generally, liability is established through national law or European law and can be derived from criminal law, civil law, or any other field of law.[16] The DSA harmonises a general horizontal liability exemption for mere conduit services, caching services, and hosting providers.[17] This article focuses exclusively on the exemption for hosting providers because of their relevance in recent case law and increased due diligence obligations in the DSA. This framework is explored in Section 2.1. Section 2.2 explains why the current consensus is that the liability exemption has not changed since the ECD, and it provides an overview of provisions that may stand in the way of interpreting the liability exemption differently. Section 2.3 provides a brief, interim conclusion.

2.1 AN OVERVIEW OF CONDITIONAL INTERMEDIARY LIABILITY EXEMPTION

The DSA's explanatory memorandum states that article 6 DSA maintains – at least textually – the liability exemption regime of article 14 ECD.[18] Article 14 ECD required Member States to ensure that hosting providers were not liable for hosting illegal content if they did not have knowledge of the illegal information they host.[19] The conditional liability exemption of Article 14 ECD was heavily inspired by paragraph 512 of the U.S. Digital Millennium Copyright Act ('DMCA'),[20] a 'sectorial, conditional immunity system'.[21] The DMCA departed from the earlier US Section 230 Communications Decency Act,[22] which immunised hosting providers from liability for hosting most types of content.[23] Immunity in paragraph 512 of the DMCA is conditional on the knowledge of the service provider of the copyright infringing content: if the service provider is unaware of copyright infringing content, they

[16] Digital Services Act (n 4) Article 3(h); Case C-291/13 *Papasavvas* EU:C:2014:2209 para 53; see also Folkert Wilman, 'The EU's System of Knowledge-Based Liability for Hosting Services Providers in Respect of Illegal User Content – Between the e-Commerce Directive and the Digital Services Act' (2021) 12(3) Journal of Intellectual Property, Information Technology and Electronic Commerce Law 317, 321.
[17] Digital Services Act (n 4) Articles 4-6.
[18] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC' COM(2020) 825 final, 3. See also Franz Hofmann and Benjamin Raue (eds), *Digital Services Act: Article-by-Article Commentary* (Nomos 2025) 162.
[19] Directive on electronic commerce (n 5) Article 14(1)(a).
[20] 17 U.S.C. para 512.
[21] Husovec, 'Rising Above Liability' (n 10) 884.
[22] 47 U.S.C. para 230.
[23] See generally Jeff Kosseff, *The Twenty-Six Words That Created the Internet* (Cornell University Press 2019).

are not liable; once made aware of such content, the service provider has to act expeditiously to remove that content. Article 14 ECD copied this model for hosting providers.[24]

The popularity of this liability exemption in the late 90s was based on the notion that less regulation would benefit economic interests and freedom of expression.[25] A framework for conditional liability exemption was seen as an agreeable middle-ground between non-liability and strict liability. Non-liability would create an undesirable situation where parties affected by illegal content are left without remedies. Conversely, strict liability would create an undesirable scenario requiring hosting providers to assume full control over all content online, which would cause unpredictable monetary loss and diminish the benefits of a decentralised communication network..[26] If hosting providers were strictly liable for illegal content, they would need to exercise immense amounts of editorial control to avoid liability. This would limit the degree to which the internet can be used for accumulating free expression, especially since various courts have recognised the internet's ability to provide a crucial vehicle for freedom of expression.[27] The downside of the liability exemption is that it leaves parties affected by illegal content with fewer remedies compared to a strict liability model, as hosting providers may hide behind being unaware of the illegal content. This is part of the balancing act that maintains the possibility of liability only if a hosting provider becomes aware of illegal content and precludes strict liability.[28] This is confirmed by the European Court of Human Rights ('ECtHR'), which held that the notice-and-action mechanism sufficiently safeguards affected parties' rights[29] – a finding that is further discussed below.[30]

The 'knowledge-based' liability exemption in Article 6 DSA – and previously Article 14 ECD – consists of three components:[31] (a) qualifying as a hosting provider; (b) not having actual knowledge of illegal content or, as regards claims for damages, not being aware of facts or circumstances from which the illegal content is apparent; or (c) acting expeditiously to remove or disable access to the illegal content.

2.1[a] Hosting providers

Hosting providers are defined in Article 3(g)(iii) DSA: 'a service consisting of the storage of information provided by, and at the request of, a recipient of the service'.[32] They must take

[24] Directive on electronic commerce (n 5) Article 14(1).
[25] See also European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on A Digital Single Market Strategy for Europe' COM(2015) 192 final, 3-4.
[26] Husovec, 'Rising Above Liability' (n 10) 893.
[27] Case C-401/19 *Commission v Poland* EU:C:2022:297 para 46; *Delfi v Estonia* (n 6) para 110; United States Supreme Court, 19 June 2017, *Packingham v North Carolina,* 137 S. Ct. 1730.
[28] E.g. Directive on electronic commerce (n 5) recitals 41 and 46; also *YouTube/Cyando* (n 6) para 113.
[29] *MTE and Index.hu v Hungary,* App no 22947/13 (ECtHR, 2 February 2016) para 91. Cf. *Delfi v Estonia* (n 6) para 159, in which the ECtHR found that in some instances action is required even without notices.
[30] See below subsection 4.1[a].
[31] Wilman, 'The EU's System of Knowledge-Based Liability for Hosting Services Providers in Respect of Illegal User Content – Between the e-Commerce Directive and the Digital Services Act' (n 16).
[32] Digital Services Act (n 4) Article 3(g)(iii); most obligations in the DSA are aimed at hosting services as opposed to mere conduit or caching services of Articles 3(g)(i) and (ii) respectively. Hosting providers have obligations under Chapter 3 Section 2; subspecies online platforms (Article 3(o)) have obligations under Section 3; online platforms allowing consumers to conclude distance contracts with traders under Section 4; and then VLOPs under Section 5; all are considered hosting providers).

a neutral role, meaning that they provide merely technical and automated processing services and do not have control over user-generated content.[33] This criterion – in the context of article 14 ECD – has been interpreted extensively in the case law of the CJEU, which has clarified how a hosting provider may interact with information while maintaining a neutral role. For example, the CJEU established in *Google France* that remuneration for hosting services does not preclude a passive role.[34] Hosting providers may also engage in indexing, searching, and recommending user-generated content.[35] However, the CJEU decided in *L'Oreal v eBay* that optimising the presentation of sales listings interfered with that neutral or passive role and excluded a hosting provider from its neutral position.[36] Neutrality of a hosting provider can therefore be seen as a spectrum, encompassing a range of activities between full passivity and full control, that has developed over time along with platform affordances that must be assessed on a case-by-case basis.[37]

2.1[b] Actual knowledge of illegal content or awareness of facts or circumstances from which illegal content is apparent

Hosting providers may not have 'actual knowledge' of illegal content or be aware of any facts or circumstances from which illegal content is apparent.[38] These are seemingly two different standards, in which actual knowledge constitutes specific knowledge of the presence of illegal content and the nature of its illegality,[39] whereas awareness of facts or circumstances from which illegal content is apparent is a broader criterion that can be derived from a broader set of circumstances.[40] The difference is that, in the case of 'awareness', liability can only lead to damages, whereas 'actual knowledge' could also lead to criminal liability.[41]

Actual knowledge or awareness of illegal content can be gained through own-initiative investigations or through notices submitted through notice-and-action mechanisms. In order to lead to awareness, notices must be sufficiently precise and adequately substantiated to allow a diligent economic operator to reasonably identify, assess,

---

[33] Digital Services Act (n 4) Article 6(2), also recital 18; *L'Oreal v eBay* (n 6) para 113. For a discussion whether neutrality also involves passiveness, see Folkert Wilman, 'Between Preservation and Clarification' (*Verfassungsblog*, 2 November 2022) <https://verfassungsblog.de/dsa-preservation-clarification/> accessed 1 September 2025.

[34] *Google France v Louis Vuitton* (n 6) para 116.

[35] Digital Services Act (n 4) recital 22; *YouTube/Cyando* (n 6) para 114.

[36] *L'Oreal v eBay* (n 6) para 116

[37] Joris van Hoboken et al, 'Hosting Intermediary Services and Illegal Content Online: An Analysis of the Scope of Article 14 ECD in Light of Developments in the Online Service Landscape' (European Commission 2018), 31–33 <https://data.europa.eu/doi/10.2759/284542> accessed 1 September 2025.

[38] It is important to note that recital 18 seemingly conflates 'being a neutral hosting provider' with 'having knowledge or control over content', stating that 'the provider of intermediary services plays an active role of such a kind as to give it knowledge of, or control over, that information'. Although there is certainly overlap between 'having actual knowledge over' and 'being aware of', it is entirely conceivable that a passive or neutral hosting provider has knowledge over illegal content.

[39] E.g. in the context of notices: Opinion of AG Saugmandsgaard Øe in Joined Cases C-682/18 and C-683/18 *YouTube/Cyando* EU:C:2020:586 para 187: 'A notification is also intended to give [the hosting provider] sufficient evidence to verify the illegal nature of the information'.

[40] Husovec, *Principles of the Digital Services Act* (n 7) 130.

[41] ibid; Miquel Peguera, 'The DMCA Safe Harbors and Their European Counterparts: A Comparative Analysis of Some Common Problems' (2008) 32(4) Columbia Journal of Law and the Arts 481, 488–489.

and where appropriate, act against illegal content.[42] The hosting provider must diligently assess the facts and circumstances brought forward in such notices.[43]

After a hosting provider has actual knowledge or awareness of allegedly illegal content, it must establish the illegal nature of the content.[44] The illegal nature must be 'a matter of actual knowledge or be apparent', meaning that the illegality must be specifically established, readily identifiable or manifest.[45] The findings of the CJEU on this are reflected in article 16(3) DSA. What is considered 'apparently' illegal can be contentious. AG Saugmandsgaard Øe comments that in some cases illegality can be immediately obvious, mentioning child abuse material as an example, whereas in others it may not be, e.g. copyright.[46] To avoid over-removal and hosting providers becoming judges of online legality, AG Saugmandsgaard Øe argues that hosting providers can only be held liable for not removing content if the illegal character of the content can be ascertained without difficulty and without conducting a detailed legal or factual examination, i.e when the illegal character is apparent.[47]

The standard for whether facts and circumstances have led to awareness of illegal content established in *L'Oreal/eBay* and in *YouTube/Cyando* is what a 'diligent economic operator' would have identified. This is a strict requirement that is not met easily: in *L'Oreal,* AG Jääskinen excludes 'construed' knowledge on the basis of the diligence expected from an economic operator, meaning that a service provider cannot be liable on the basis of that they 'should have known', or whether they 'have good reasons to suspect illegal activity'.[48] Expecting otherwise could violate the prohibition on general monitoring obligations under article 15 ECD and 8 DSA. However, Jääskinen nuances this finding for 'same or similar' trademark infringing goods, arguing that 'same or similar' infringements are part of the same illegal activity and, as such, constitute 'ongoing' illegal content, in which case the provider 'should have known' of the trademark infringement.[49]

The Court finds in *L'Oreal* that an imprecise or inadequately substantiated notice must be taken into account by national courts in establishing whether there are facts and circumstances from which a diligent economic operator should have identified the illegal content.[50] Nordemann interprets this as a duty of care, requiring some effort of the economic operator to identify illegal content based on facts presented to them.[51] *YouTube* nuances this finding. AG Saugmandsgaard Øe seemingly dismisses the argument that awareness can be construed on the basis of the expected diligence or duty of care of an operator, stating: 'attention should be paid not to the fact that the provider would have known had it been

---

[42] Digital Services Act (n 4) recital 22; Article 16(3).
[43] ibid Article 16(6)
[44] *Google France v Louis Vuitton* (n 6) para 109. See also Hofmann and Raue (n 18) 170.
[45] *YouTube/Cyando* (n 6) para 113.
[46] Opinion of AG Saugmandsgaard Øe in *YouTube/Cyando* (n 39) paras 187-190. Saugmandsgaard Øe argues that copyright cases can be difficult to assess due to the variety of rightholders that can be involved and the various national regimes that may need to be accounted for, referring explicitly Case C-360/10 *SABAM v Netlog* EU:C:2012:85 para 50. However, copyright cases have also been dubbed some of the more obvious cases of illegal content; in cases of piracy, illegality is often clear-cut.
[47] Opinion of AG Saugmandsgaard Øe in *YouTube/Cyando* (n 39) para 190.
[48] Opinion of AG Jääskinen in Case C-324/09 *L'Oreal v eBay* EU:C:2010:757 para 163.
[49] ibid para 167.
[50] *L'Oreal v eBay* (n 6) para 122.
[51] Jan Bernd Nordemann, 'Haftung von Providern im Urheberrecht Der aktuelle Stand nach dem EuGH-Urteil v. 12. 7. 2011 – C-324/09 – L'Oréal/eBay' [2011] GRUR 977.

diligent, but to what it really knew'.[52] The final decision in *YouTube* confirms this line of reasoning, finding that the notification must contain sufficient information to enable the operator to satisfy itself without a detailed legal examination that the content is illegal and that removing it is compatible with freedom of expression.[53] Thus, there is limited room in case law for a duty of care, and only in certain circumstances.

The level of diligence required from the 'diligent economic operator' is left relatively undefined unclear throughout this development. Adding to this complexity, Saugmandsgaard Øe links the liability exemption of article 14 ECD to the concept of good faith. Citing the input by the French Government, he finds that the liability exemption 'seeks to protect service providers that generally act in good faith, not providers whose very intention is to facilitate copyright infringements'.[54] Good faith can be demonstrated through generally complying with obligations to remove content, or by putting in place tools that combat illegal content.[55] However, judging by the tone of the CJEU[56] and the AG[57], it is interpreted primarily as a criterion of *neither* deliberately facilitating illegal content nor remaining inactive despite having general awareness of the hosting service being used to disseminate illegal content.

2.1[c] Acts expeditiously to remove access to the illegal content

Upon having gained actual knowledge or awareness of illegal content, a hosting provider must act expeditiously to remove or disable access to the illegal content. This involves both a temporal requirement – content must be removed expeditiously – and the question of whether the platform could be required to remove content that is identical or similar to the illegal content.

The requirement of 'expedience' is undefined and needs to be assessed on a case-by-case basis.[58] It can be dependent on the nature of the content: for example, the expected expedience for removing CAM ('Child Abuse Material') may be greater than that of unwarranted financial advice. The requirement for member states is that temporal requirements may not be so rigid as to inspire over-blocking.[59] Previously, the *Conseil Constitutionnel* found that removal times under 24 hours in *Loi Avia* were unconstitutional as they may lead platforms to remove content even in cases of doubt.[60] In contrast, the 2025 Code of Conduct on Countering Illegal Hate Speech Online+ requires signatories

[52] Opinion of AG Saugmandsgaard Øe in *YouTube/Cyando* (n 39) para 179; referring to Opinion of AG Jääskinen in *L'Oreal v eBay* (n 48) para 163.
[53] *YouTube/Cyando,* (n 6) para 116, also Opinion of AG Saugmandsgaard Øe in *YouTube/Cyando* (n 39) para 190.
[54] Opinion of AG Saugmandsgaard Øe in *YouTube/Cyando* (n 39) fn. 187.
[55] Opinion of AG Saugmandsgaard Øe in *YouTube/Cyando* (n 39) paras 124 and 128.
[56] *YouTube/Cyando* (n 6) para 94 on YouTube having various measures to prevent copyright infringement, and para 98, on Cyando not facilitating illegal sharing.
[57] Opinion of AG Saugmandsgaard Øe in *YouTube/Cyando* (n 39) para 191.
[58] Digital Services Act (n 4) recital 52; see also Hofmann and Raue (n 18) 178-179.
[59] Benjamin Raue and Hendrik Heesen, 'Raue/Heesen: Der Digital Services Act' [2022] Neue Juristische Wochenschrift 3537, 3540.
[60] *Conseil Constitutionnel,* 18 June 2020, 2020-801 DC, para 16; see Ruth Janal, 'Haftung Und Verantwortung Im Entwurf Des Digital Services Acts' [2021] Zeitschrift für Europäisches Privatrecht 227, 248.

to review 50% of notices of illegal hate speech online within 24 hours.[61] The absolute time requirements posed by Article 6(1)(b) DSA for takedown therefore remain somewhat vague, but in its Code of Conduct the Commission shows tolerance for stricter removal times.

Article 6(1)(b) DSA also raises the question of whether awareness of specific illegal content could lead to an obligation to remove identical or similar content: can hosting providers be required to ensure *staydown* instead of *takedown*?[62] Staydown implies that future infringements must also be removed, which may require the hosting provider to moderate content *ex ante*. The notice-and-staydown model is popular in cases of copyright infringement: for example, under the German doctrine of *Störerhaftung*, injunctions could be ordered for future infringing materials.[63] However, monitoring for similar infringements creates a tension with the general monitoring prohibition of Article 8 DSA, as it would require hosting providers to proactively monitor content.

This tension is resolved somewhat inconsistently in CJEU case law over the past decade. In *Scarlet v SABAM* and *SABAM v Netlog*, the CJEU found that requiring preventive monitoring of all data by an internet service provider for intellectual property infringing content would contravene the general monitoring obligation of Article 15(1) ECD.[64] In *McFadden* this reasoning was confirmed.[65] Conversely, in *L'Oréal,* the CJEU finds that injunctions to suspend violators of intellectual property rights may be ordered if operators of online marketplaces fail to take preventive measures, which encourages some forms of proactive content moderation.[66] The CJEU nuances this line in *Glawischnig-Piesczek v Facebook*: it is not considered a general monitoring obligation when a hosting providers are required to remove identical – as already established in *L'Oreal* – and similar content.[67] The qualification 'similar' is novel. In *Glawischnig-Piesczek,* it is required by the nature of defamatory content, which may take different forms, but be similar at its core.[68] Similarity can only be established when it does not require an independent assessment by the hosting provider.[69] Janal argues that removing 'similar' content inevitably requires the use of filtering techniques, yet filtering may not lend themselves to effectively judging the context in which the defamatory speech is uttered. This may then contravene article 8 DSA.[70] To add a layer of proportionality to this requirement of filtering for similar content, A-G Saugmandsgaard Øe argues in his conclusion in *YouTube* that, if monitoring obligations for identical or similar content are ordered, those obligations must be proportionate to the complexity of the obligation (i.e.

[61] European Commission, 'Code of conduct on Countering Illegal Hate Speech Online +' (20 January 2025), 2.3 <https://digital-strategy.ec.europa.eu/en/library/code-conduct-countering-illegal-hate-speech-online> accessed 1 September2025.
[62] Martin Husovec, 'The Promises of Algorithmic Copyright Enforcement: Takedown or Staydown? Which Is Superior? And Why?' (2018) 42(1) Columbia Journal of Law & the Arts 53. Also Aleksandra Kuczerawy, 'From "Notice and Takedown" to "Notice and Stay Down": Risks and Safeguards for Freedom of Expression' in Giancarlo Frosio (ed), *Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020).
[63] E.g. *Bundesgerichtshof,* 12 March 2004, *Internetversteigerung I,* I ZR 304/01; see for example Christina Angelopoulos and Stijn Smet, 'Notice-and-Fair-Balance: How to Reach a Compromise between Fundamental Rights in European Intermediary Liability' (2016) 8(2) Journal of Media Law 266, 285; Kuczerawy, 'From "Notice and Takedown" to "Notice and Stay Down"' (n 62) 540.
[64] Case C-70/10 *Scarlet Extended v SABAM* EU:C:2011:771 paras 39-40; *SABAM v Netlog* (n 46).
[65] Case C-484/14 *Tobias McFadden v Sony Music Entertainment* EU:C:2016:689 para 87.
[66] *L'Oreal v eBay* (n 6) para 141.
[67] Case C-18/18 *Eva Glawischnig-Piesczek v Facebook* EU:C:2019:821 para 37.
[68] ibid para 40.
[69] ibid para 46.
[70] Janal (n 60) 249-250.

similar content is more difficult to monitor than identical content) and, therefore, take into account the availability of monitoring systems to the hosting provider.[71] In sum, the CJEU does not fully dismiss the possibility of near-general monitoring obligations, but these need to be necessitated by the nature of the illegal content and proportional to the situation of the hosting provider.

2.1[d] Limitations to the scope of applicability of the liability exemption under article 6(1) DSA.

The DSA limits liability exemption compared to Article 14 ECD in two instances: in Article 6(3) and by leaving sectoral regulation on illegal content that creates different standards for liability exemption (e.g. the Copyright in the Digital Single Market Directive ('CDSM'))[72] intact.

Article 6(3) DSA stipulates that liability under consumer protection cannot be exempted for online platforms that allow the conclusion of distance contracts with traders where the average consumer could believe that the product was sold by the online platform itself.[73] This answers a critique that hosting providers are not liable for consumer harms even though consumers rely on the hosting provider's brand image to buy goods and services.[74] Sectoral regulation fragments the landscape of intermediary liability exemption for illegal content outside of the DSA's scope. The Copyright Directive,[75] Enforcement Directive[76] and CDSM Directive all act as *leges speciales* under the DSA.[77] Under the CDSM Directive online content-sharing service providers[78] perform an act of communicating to the public when hosting third-party content.[79] If they host copyright infringing content, they must obtain prior authorisation from right-holders to do so or face liability for copyright infringement.[80] Providers may be exempt from liability if they (a) made best efforts to obtain authorisation; (b) made, in accordance with high industry standards of professional diligence, best efforts to ensure the unavailability of specific works; and (c) acted expeditiously to remove content upon receiving a notification and made best efforts to remove future uploads.[81] This is a higher standard of liability exemption than Article 6 DSA, which is justified by addressing right-holders from a value-gap created by negligent enforcement on behalf of online service

[71] Opinion of AG Saugmandsgaard Øe in *YouTube/Cyando* (n 39) para 222.
[72] Directive 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market [2019] OJ L130/92.
[73] Digital Services Act (n 4) Article 6(3).
[74] E.g. Caroline Cauffman and Catalina Goanta, 'A New Order: The Digital Services Act and Consumer Protection' (2021) 12(4) European Journal of Risk Regulation 758, 766–767. Caufman and Goanta criticise the provision (then Article 5(3) of the DSA proposal) for creating legal uncertainty on the interpretation of average consumer – although that is a common standard in consumer law, it is still unclear what factors lead an average consumer to assume that the hosting provider is party to the contract.
[75] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society [2001] OJ L167/10.
[76] Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights [2004] OJ L157/45.
[77] Digital Services Act (n 4) recital 11.
[78] Directive 2019/790 (n 72) Article 2(6); this can bes een as a subset of online platforms in the sense of Article 3(i) DSA.
[79] Directive 2001/29 (n 75) Article 3.
[80] Directive 2019/790 (n 72) Article 17(1); Directive 2001/29 (n 75) Article 3.
[81] Directive 2019/790 (n 72) Article 17(4).

providers.[82] To be exempt from liability in the case of copyright, online platforms may be required to employ automated filtering techniques,[83] creating a tension with Article 8 DSA and generally the right to freedom of expression.[84] The CJEU resolved this tension in *Poland v Commission,* finding that platforms are not obliged to generally monitor and that Article 17(7)-(9) provides sufficient safeguards to balance copyright and the right to freedom of expression.[85]

2.2 WHY IS THE CONSENSUS THAT THE HOSTING LIABILITY EXEMPTION HAS NOT CHANGED?

As iterated above, the academic consensus is that the framework for liability exemption has not changed since the ECD. The fundamental reasoning behind the liability exemption – balancing the promotion of economic development in internet services, maintaining freedom of expression by not mandating general monitoring for all illegal content and offering users a remedy via notice-and-action and potential liability – remains intact.[86] Most reports evaluating the intermediary liability exemption generally find that, although the ECD required clarification, there was no real support for fundamentally altering the liability exemption.[87] The liability exemption regime was considered 'fit-for-purpose' by most individual users, content uploaders, and intermediaries.[88] Only IP-rightholders indicate flaws in both the system and its interpretation in case law, stating it does not allow them sufficient redress from intermediaries and infringing parties. Their

[82] Directive 2019/790 (n 72) recital 66. Cf. on whether this justifies stricter liability than in other fields, Janal (n 60) 235-236.
[83] Christophe Geiger and Bernd Justin Jütte, 'Platform Liability Under Art. 17 of the Copyright in the Digital Single Market Directive, Automated Filtering and Fundamental Rights: An Impossible Match' (2021) 70(6) GRUR International 517, 550–552.
[84] This provision has been popular topic of academic debate, see for example: Geiger and Jütte (n 83); João Pedro Quintais et al, 'Safeguarding User Freedoms in Implementing Article 17 of the Copyright in the Digital Single Market Directive Statements' (2019) 10(3) Journal of Intellectual Property, Information Technology and Electronic Commerce Law 277; Martin Husovec, 'Mandatory Filtering Does Not Always Violate Freedom of Expression: Important Lessons from *Poland v. Council and European Parliament*' (2023) 60(1) Common Market Law Review 173; Martin Senftleben and Christina Angelopoulos, 'The Odyssey of the Prohibition on General Monitoring Obligations on the Way to the Digital Services Act: Between Article 15 of the e-Commerce Directive and Article 17 of the Directive on Copyright in the Digital Single Market' (*SSRN*, 4 January 2021) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3717022> accessed 1 September 2025.
[85] *Commission v Poland,* (n 27) paras 72-97.
[86] Generally, Wilman, 'The EU's System of Knowledge-Based Liability for Hosting Services Providers in Respect of Illegal User Content – Between the e-Commerce Directive and the Digital Services Act' (n 16) 322-323.
[87] E.g. van Hoboken et al (n 37); Gellert and Wolters (n 5); Tambiama Madiega, 'Reform of the EU Liability Regime for Online Intermediaries: Background on the Forthcoming Digital Services Act : In Depth Analysis.' (European Parliament 2019, PE 649.404) <https://data.europa.eu/doi/10.2861/08522> accessed 1 September 2025; Anja Hoffmann and Alessandro Gasparotti, 'Liability for Illegal Content Online' (Centre for European Policy, March 2020) <https://www.cep.eu/fileadmin/user_upload/hayek-stiftung.de/cepStudy_Liability_for_illegal_content_online.pdf> accessed 1 September 2025.
[88] European Commission, 'Synopsis report on the public consultation on the regulatory environment for platforms, online intermediaries and het collaborative economy' (2015) <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=15877> accessed 1 September 2025; see also Maria Lillà Montagnani, 'A New Liability Regime for Illegal Content in the Digital Single Market Strategy' in Giancarlo Frosio (ed), *The Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020).

concerns have been addressed in Directive 2019/790.[89]

Instead, the DSA adds a layer of accountability norms in the form of due diligence and transparency, which are not linked to liability. Husovec calls this 'accountability-but-not-liability'.[90] These provisions require additional efforts from platforms but do not translate to intermediary liability. This separation may stand in the way of a more narrow interpretation of the liability exemption in the DSA compared to the ECD. This subsection describes some provisions that would stand in the way of a more narrow interpretation of the liability exemption.

The first provision anchoring liability exemption amidst other norms is Article 54. It explicitly separates liability for hosting illegal content from liability for individual harms suffered by infringement of the DSA.[91] The reasoning behind this distinction is that liability for illegal content is aimed at restoring a lawful state by making victims whole, whereas liability under Article 54 is only about holding platforms accountable for complying with their obligations under the DSA.[92] Accountability provisions in the DSA on transparency and due diligence are therefore not intended create liability for the communication of others.[93] Recital 41 underscores this sentiment: 'the due diligence obligations are independent from the question of liability of providers of intermediary services, which therefore need to be assessed separately'.[94] To clarify this separation with an example, it is impossible to hold a platform for hosting CAM because it was late in submitting transparency reporting.[95] Since a separate avenue for liability for the novel obligations stemming from the DSA's due diligence system is available, it is not necessary to link the doctrine for intermediary liability exemption to the due diligence system.

A second provision preventing a narrow reading of liability exemption is the Good Samaritan provision of Article 7.[96] Article 7 confirms that intermediary service providers are not excluded from relying on liability exemptions of Articles 4-6 DSA if they carry out voluntary good faith investigations into illegal content or take necessary measures to comply with national or EU law, and if this also leads to an active or non-neutral role that would normally exclude them from qualifying as a hosting provider. This provision prevents a catch-22 in which an online platform would be excluded from the liability exemption because they moderate content in good faith.[97] Exclusion from liability exemption for good faith

[89] Directive 2019/790 (n 72). See Section 2.3; also more extensively João Pedro Quintais and Sebastian Felix Schwemer, 'The Interplay between the Digital Services Act and Sector Regulation: How Special Is Copyright?' (2022) 13(2) European Journal of Risk Regulation 191.
[90] Husovec, 'Rising Above Liability' (n 10) 910. See also Giancarlo Frosio and Martin Husovec, 'Accountability and Responsibility of Online Intermediaries' in Giancarlo Frosio (ed), *The Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020).
[91] Digital Services Act (n 4) Article 54.
[92] Husovec, 'Rising Above Liability' (n 10) 911.
[93] Husovec, *Principles of the Digital Services Act* (n 7) 66.
[94] Digital Services Act (n 4) recital 41.
[95] Hofmann and Raue (n 18) 958-960.
[96] Digital Services Act (n 4) Article 7.
[97] van Hoboken et al (n 37) 39. This fear was not justified even without the Good Samaritan provision, see e.g. Directive on electronic commerce (n 5) recital 40; European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Tackling Illegal Content Online' COM(2017)555 final, 12-13; see also Gellert and Wolters (n 5) 68-69.

content moderation could lead to less moderation to avoid liability.[98] Good faith implies that platforms operate in an objective, non-discriminatory and proportionate manner and take into account the rights and legitimate interests of all the parties involved.[99] The application of the Good Samaritan provision may be limited by the requirement of diligence, critics argue. Berbec, referring to Kuczerawy, questions whether the liability exemption is available, for example, if a hosting provider only succeeds in removing some illegal content on the basis of a notice, but misses some identical or similar content of which the illegal nature is apparent.[100] An undiligent hosting provider may therefore be excluded from the provision, leading to the conclusion that 'taking voluntary actions in good faith neither guarantees no[r] precludes neutrality'.[101] In spite of this, the article is commonly seen as an assurance that platforms should moderate content without fearing lability, and therefore ensures that the liability exemption also extends to hosting providers that actively moderate content.[102]

A final limitation is laid down in Article 8 DSA, which prohibits general monitoring obligations.[103] The ECD allowed for member states to create explicit duties of care regarding certain types of illegal content.[104] The DSA does not copy this, making the general monitoring prohibition stricter.[105] General monitoring obligations are prohibited due to operational costs for hosting providers and risks to the freedom of expression. The use of automated filtering is associated with risks to freedom of expression because of the potential for catching proverbial 'dolphins in the net', where legal content is inadvertently removed.[106] Article 8 must be interpreted as precluding any level of diligence being expected of an operator that may lead to a *de facto* or *de jure* general monitoring obligation or pro-active measures relating

[98] By analogy: 'where ignorance is bliss, "tis wise to be folly"', California Court of Appeals, June 23 1958, *People v Smith*, Civ. A. No. 3792.
[99] Digital Services Act (n 4) recital 26, see also Jacob van de Kerkhof, 'Good Faith in Article 6 Digital Services Act (Good Samaritan Exemption)' (*The Digital Constitutionalist*, 15 February 2023) <https://digi-con.org/good-faith-in-article-6-digital-services-act-good-samaritan-exemption/> accessed 1 September 2025.
[100] Adriana Berbec, 'To What Extent Can Online Service Providers Adopt Voluntary Content Moderation Measures without Losing Their Immunity Shields? A Comparative Analysis of Online Service Providers' Liabilities in the European Union and the United States' (2024) 15(1) Journal of Intellectual Property, Information Technology and E-Commerce Law 13; Aleksandra Kuczerawy, 'The Good Samaritan That Wasn't: Voluntary Monitoring under the (Draft) Digital Services Act' (*Verfassungsblog*, 12 January 2021) <https://verfassungsblog.de/good-samaritan-dsa/> accessed 1 September 2025; the requirement to moderate against content of which the illegal nature is apparent arises from Opinion of AG Saugmandsgaard Øe in *YouTube/Cyando* (n 39) para 197.
[101] Kuczerawy, 'The Good Samaritan That Wasn't' (n 100).
[102] Wilman, 'The EU's System of Knowledge-Based Liability for Hosting Services Providers in Respect of Illegal User Content – Between the e-Commerce Directive and the Digital Services Act' (n 16) 335. Unclear: *YouTube/Cyando* (n 6) para 109.
[103] Digital Services Act (n 4) Article 8; previously included as Article 15 in Directive on electronic commerce (n 5).
[104] Directive on electronic commerce (n 5) recital 48.
[105] Arguably, the explicit duties of care are included in sectoral regulation, see e.g. Gerald Spindler, 'The Liability System of Art. 17 DSMD and National Implementation: Contravening Prohibition of General Monitoring Duties' (2019) 10(3) Journal of Intellectual Property, Information Technology and Electronic Commerce Law 344; Senftleben and Angelopoulos (n 84).
[106] E.g. Daphne Keller, 'Dolphins in the Net: Internet Content Filters and the Advocate General's Glawischnig-Piesczek v. Facebook Ireland Opinion' (Stanford Center for Internet and Society, 4 September 2019) <https://cyberlaw.stanford.edu/content/files/2024/05/Dolphins-in-the-Net-AG-Analysis.pdf> accessed 1 September 2025; more generally: Robert Gorwa, Reuben Binns and Christian Katzenbach, 'Algorithmic Content Moderation: Technical and Political Challenges in the Automation of Platform Governance' (2020) 7(1) Big Data & Society 1.

to identifying or monitoring illegal content.[107] Specific monitoring obligations are allowed for similar or identical content, however, following *Glawischnig-Piesczek*.[108] *De facto* general monitoring obligations are created by assuming a duty of care that is too expansive. Article 8 DSA can therefore stand in the way of limiting the liability exemption: by making hosting providers more liable, providers are *de facto* expected to assume a more active role in content moderation, which is precluded by Article 8.

2.3 INTERMEDIARY FINDINGS

This Section has presented an overview of the intermediary liability exemption in Article 6 DSA. Neutral intermediary service providers are not liable for hosting illegal content if they have no specific knowledge of that content or its illegality, and if they act expeditiously to remove it after gaining knowledge. The liability exemption for hosting providers is justified by facilitating economic growth of digital service providers and ensuring that freedom of expression is not interfered with through over-removing content by hosting providers fearing liability. Despite the added responsibility for hosting providers codified in the DSA and sector-specific regulation, the liability exemption has not significantly changed since the e-Commerce Directive of 2000. Its scope is somewhat limited by Article 6(3) DSA and sectoral regulation, but its key characteristics remain. In fact, altering the scope of the liability exemption in the DSA is prevented by the Good Samaritan provision of Article 7 DSA, the separate ground for liability of Article 54 DSA, and the general monitoring prohibition of Article 8 DSA. However, this article argues that there is room for a nuanced rethinking of the intermediary liability exemption guided by provisions in the DSA. Section 3 outlines arguments that justify narrowing of the scope of intermediary liability exemption within the framework of the DSA. This rethinking does not dismiss the key characteristics of the liability exemption, but ensures that it applies to good faith actors whilst excluding bad faith hosting providers.

3 WHY SHOULD WE RETHINK THE INTERMEDIARY LIABILITY EXEMPTION OF ARTICLE 6 DSA?

This article contests that the DSA allows for the liability exemption to be interpreted more narrowly than it was under the ECD, at least on a case-by-case basis. In some instances, this could aid individual aggrieved parties and rightholders with an additional remedy vis-à-vis the platform, which is currently precluded by a broad liability exemption. Aside from the general observation that laws applying to the internet drafted in the year 2000 may not be entirely fit for a fast-developing digital economy, this contestation rests on five points: (i) insufficient access to functioning notice-and-action mechanisms warrants a narrower application of the liability exemption; (ii) a narrower exemption would reflect a fairer division of the economic burden of moderation; (iii) a narrower liability exemption reflects developments in moderation capacity over the past two decades; (iv) a narrower exemption could contravene a geopolitical interest in less moderation and create enforcement mechanisms against mis-moderation; and (v) the case law of the European Court of Human

[107] Digital Services Act (n 4) recital 22.
[108] *Eva Glawischnig-Piesczek v Facebook* (n 67).

Rights indicates that the freedom of expression does not necessarily preclude a stricter liability exemption.

3.1 INSUFFICIENT ACCESS TO FUNCTIONING NOTICE-AND-ACTION MECHANISMS

Notice-and-action mechanisms of online platform providers constitutes a cornerstone in the intermediary liability exemption structure outlined in Section 2.1. Liability exemption can – at least under the ECD and DSA – only be justified if parties aggrieved by illegal content have a remedy available. That remedy is provided by an avenue for the affected party to request takedown of the illegal content. This is usually achieved through a notice-and-action mechanism. The importance of such mechanisms is acknowledged by the EU regulator,[109] the ECtHR in *MTE v Hungary* (finding that a functioning notice-and-action mechanism acts as a balancing instrument between various interests, and would thus not justify liability for hosting comments),[110] and the CJEU (in acknowledging the importance of notice-and-action mechanisms in combatting copyright infringements in *Youtube/Cyando*).[111] National case law also emphasises the importance of such mechanisms in facilitating users to act against illegal content.[112]

Previously, the requirements for notice-and-action were fragmented on a member state level.[113] The DSA progresses this thorny issue in harmonising those requirements, explicitly acknowledging that (a) hosting providers must provide their users with an easily accessible and user-friendly means of reporting content;[114] and (b) that a notice through such as mechanism creates knowledge or awareness of illegal content with the hosting provider, thus excluding them from liability exemption if they do not act expeditiously.[115]

The design of such mechanisms greatly affects how users are able to submit notices. Several studies have indicated that hosting providers do not adhere to requirements of ease-of-access or user-friendliness. In works on Germany's *Netzwerkdurchsetzungsgesetz,* which also included a notice-and-takedown requirement, Heldt[116] and Wagner et al[117] show that Facebook's design of their notice-and-action mechanism affects how users report content. The reporting affordance for illegal content was considerably less accessible than that for incompliance with terms and conditions, resulting in users submitting less notices on illegal

---

[109] Commission, 'Communication on Tackling Illegal Content Online' (n 97) 16.
[110] *MTE and Index.hu v Hungary* (n 29) para 91.
[111] *YouTube/Cyando* (n 6) para 94.
[112] E.g. Hoge Raad, 27 January 2023, *Brein v NSE,* ECLI:NL:HR:2023:94 para 1.4 et seq.
[113] Aleksandra Kuczerawy, 'Intermediary Liability & Freedom of Expression: Recent Developments in the EU Notice & Action Initiative' (2015) 31(1) Computer Law & Security Review 46, 51.
[114] Digital Services Act (n 4) Article 16(1).
[115] ibid Article 16(3).
[116] Amélie Heldt, 'Reading between the Lines and the Numbers: An Analysis of the First NetzDG Reports' (2019) 8(2) Internet Policy Review <https://policyreview.info/articles/analysis/reading-between-lines-and-numbers-analysis-first-netzdg-reports> accessed 1 September 2025.
[117] Ben Wagner et al, 'Regulating Transparency?: Facebook, Twitter and the German Network Enforcement Act' (Proceedings of the 2020 ACM Conference on Fairness, Accountability, and Transparency, Association for Computing Machinery 2020) <https://dl.acm.org/doi/10.1145/3351095.3372856> accessed 1 September 2025.

content. Sekwenz et al[118] and Holznagel[119] observe a similar trend regarding Article 16 DSA notice-and-action mechanisms for TikTok and Facebook: notice-and-action mechanisms are poorly implemented, leading to users being dissuaded from reporting illegal content, or not being able to report it as illegal. Article 16 has led to various complaints against VLOPs.[120] If the avenue for generating knowledge or awareness of illegal content with the hosting provider is dysfunctional, hosting providers remain within the scope of the liability exemption, since it is more difficult to create awareness of illegal content. Non-compliance with Article 16 can therefore, to some extent, be rewarding; the user is less able to alert the platform and therefore trigger liability. The only remedy currently for individuals against this is Article 54 DSA. However, if functioning notice-and-action mechanisms are a precondition for liability exemption, it seems plausible that not providing such mechanisms could lead to exclusion from the liability exemption, as is argued in subsection 4.1[a].

3.2 FAIRER ECONOMIC BURDEN FOR HOSTING ILLEGAL CONTENT

Narrowing liability exemption can be justified because it requires internet intermediaries, who generally benefit economically from hosting illegal content, to be accountable to parties seeking a remedy when affected by illegal content. Buiten et al have conducted a law and economics analysis of liability rules for hosting services.[121] Their analysis starts with the observation that hosting providers are stuck in a paradox where they may want to act against illegal content online but simultaneously profit from the presence of that content on their services. Since they benefit economically from hosting content, it is fair to place responsibility for the costs of content moderation with those hosting providers. Their economic benefit can also be used as an argument for holding them liable: '[i]f hosting platforms reap the benefits from exchange in the space they govern, it stands to reason that they also face responsibility if their business model causes harm'.[122] Their analysis is supported by the so-called 'value-gap'. The 'value gap' is a term coined by copyright holders to describe the situation in which the hosting provider generates income over infringing content but the original rightsholder does not.[123] The CDSM Directive addresses the value gap for copyright

[118] Marie-Therese Sekwenz, Ben Wagner, and Simon Parkin, "'It Is Unfair, and It Would Be Unwise to Expect the User to Know the Law!" – Evaluating Reporting Mechanisms under the Digital Services Act' (Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency, Association for Computing Machinery 2025) <https://dl.acm.org/doi/10.1145/3715275.3732036> accessed 1 September 2025.
[119] Daniel Holznagel, 'Follow Me to Unregulated Waters!' (*Verfassungsblog*. 30 May 2024) <https://verfassungsblog.de/follow-me-to-unregulated-waters/> accessed 1 September 2025.
[120] E.g. TikTok: HateAid, 'HateAid Files a Complaint against TikTok' (*HateAid*, 14 February 2025) <https://hateaid.org/en/systemic-failure-hateaid-files-complaint-against-tiktok/> accessed 1 September. Also Meta: European Commission, 'Commission Opens Formal Proceedings under DSA' (*European Commission*, 30 April 2024) < https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2373 > accessed 1 September 2025.
[121] Miriam C Buiten, Alexandre de Streel, and Martin Peitz, 'Rethinking Liability Rules for Online Hosting Platforms' (2020) 28(2) International Journal of Law and Information Technology 139.
[122] ibid 149.
[123] Annemarie Bridy, 'The Price of Closing the "Value Gap": How the Music Industry Hacked EU Copyright Reform' (2020) 22(2) Vanderbilt Journal of Entertainment & Technology Law 323.

holders through a stricter liability regime.[124] However, the internet economy has developed beyond generating income through copyright infringing content, but other content remains under a 'loose' liability exemption regime. Users – and therefore hosting providers – also generate income by defaming people, or spreading hatred.[125] The negative effects – material and immaterial – of such speech are not carried by the platform, however; they are carried by citizens. It could be considered a fairer distribution of the burden for hosting illegal content if bad faith actors profiting monetarily from hosting illegal content would be excluded from liability exemption, allowing aggrieved parties to hold them liable.

3.3 IMPROVED MODERATION CAPACITY

Content moderation processes have improved significantly since the early 2000s due to advances in automation. Automation is necessitated by the enormous scale on which content is moderated.[126] Hosting providers have since developed sophisticated tools to automate content moderation.[127] To illustrate, every 6 months roughly 10 billion content moderation decisions are uploaded into the DSA Transparency Database, the vast majority of which are automated.[128] Academic discourse has focused primarily on weaknesses in automated procedures regarding freedom of expression[129] and transparency;[130] however, it is undeniable that content moderation has advanced significantly, especially since human moderation is also not an absolute guarantee of accuracy. It is expected that advancements in the use of large language models in content moderation will add to content moderation accuracy in the future.[131]

The increased accuracy of content moderation since the early 2000s leads to higher detection and higher removal rates of illegal content: a development that is boasted by the largest social media platforms, who increasingly rely on automated moderation at the expense

---

[124] Martin Senftleben, João Pedro Quintais, and Arlette Meiring, 'How the EU Outsources the Task of Human Rights Protection to Platforms and Users: The Case of UGC Monetization' (2023) 38(3) Berkeley Technology Law Journal 101, 105.

[125] Thales Bertaglia, Catalina Goanta, and Adriana Iamnitchi, 'The Monetisation of Toxicity: Analysing YouTube Content Creators and Controversy-Driven Engagement' (4th International Workshop on Open Challenges in Online Social Networks, Association for Computing Machinery 2024) <https://dl.acm.org/doi/10.1145/3677117.3685005> accessed 1 September 2025.

[126] Tarleton Gillespie, 'Content Moderation, AI, and the Question of Scale' (2020) 7(2) Big Data & Society 1.

[127] For example: European Commission, 'Working Document Impact Assessment on the Modernisation of the EU Copyright Rules' SWD(2016) 301 final.

[128] Amaury Trujillo, Tiziano Fagni, and Stefano Cresci, 'The DSA Transparency Database: Auditing Self-Reported Moderation Actions by Social Media' (2025) 9(2) Proceedings of the ACM on Human-Computer Interaction 1; Rishabh Kaushal et al, 'Automated Transparency: A Legal and Empirical Analysis of the Digital Services Act Transparency Database' (The 2024 ACM Conference on Fairness, Accountability, and Transparency) <https://dl.acm.org/doi/10.1145/3630106.3658960> accessed 1 September 2025.

[129] E.g. Federica Casarosa, 'When the Algorithm Is Not Fully Reliable: The Collaboration between Technology and Humans in the Fight against Hate Speech' in Hans-W Micklitz et al (eds), *Constitutional Challenges in the Algorithmic Society* (Cambridge University Press 2021); Céline Castets-Renardt, 'Algorithmic Content Moderation on Social Media in EU Law: Illusion of Perfect Enforcement' (2020) 2020(2) University of Illinois Journal of Law Technology & Policy 283.

[130] E.g. Mike Ananny and Kate Crawford, 'Seeing without Knowing: Limitations of the Transparency Ideal and Its Application to Algorithmic Accountability' (2018) 20(3) New Media & Society 973; Lilian Edwards and Michael Veale, 'Slave to the Algorithm? Why a Right to an Explanation Is Probably Not the Remedy You Are Looking For' (2017) 16(1) Duke Law & Technology Review 18.

[131] E.g. Emmanuel Vargas Penagos, 'ChatGPT, Can You Solve the Content Moderation Dilemma?' (2024) 32 International Journal of Law and Information Technology eaae028.

of human moderation.[132] Their boasting of successful moderation processes also raises expectations. The expectation of accuracy is underlined in several (co-)regulatory documents, for example the Code of Conduct+[133] against illegal hate speech and the Regulation on terrorist content online.[134] Although Article 7 DSA precludes such good faith investigations leading to liability (see Section 2.2), the expected accuracy created by social media networks' own PR, as well as the evolvement of content moderation into a sophisticated process, should factor in assessing liability exemption under Article 6. Not only will the advancement of content moderation lead to awareness of illegal content on a factual basis more frequently, it also raises the question whether platforms choosing not to apply such measures should be held liable for negligence.[135] Of course, it is a conscious choice of the EU regulator not to mimic the liability exemption of the CDSM Directive. However, the DSA's liability exemption stems from a period in time when it was impossible for hosting providers to control all content. Even though this is even more true nowadays due to the exponential growth of hosting services, automation and sophistication do allow hosting providers to better control content. This requires rethinking whether hosting providers should be exempt from liability even if they have advanced methods available – especially in cases where they choose not to use such methods.

3.4 PROVIDING A COUNTERMOVEMENT TO A TREND OF MODERATION WITHDRAWAL

As illustrated by the anecdote in the introduction, it is not uncommon for intermediary service providers to make mistakes in content moderation. This is not problematic per se, most platform regulations acknowledge that perfect moderation is impossible.[136] However, the current political climate in the United States supports reducing content moderation efforts. Protected by the geopolitical influence of the Trump administration, which is publicly threatening the EU if it applies the DSA too stringently,[137] CEO's of online platforms increasingly move towards less moderation.[138] This means that the dissemination of illegal content online increases. As an example, the prevalence of hate speech on X has increased significantly since Musk became its CEO.[139]

Intermediary liability can be an effective incentive for hosting providers to remove illegal content more actively. Liability needs to be weighed against the risks to freedom of

---

[132] Latiff (n 2); 'Meta's New AI System to Help Tackle Harmful Content' (*Meta Newsroom*, 8 December 2021) <https://about.fb.com/news/2021/12/metas-new-ai-system-tackles-harmful-content/> accessed 1 September 2025.

[133] Code of conduct on Countering Illegal Hate Speech Online + (n 61) Article 4.2.4.

[134] Regulation 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online [2021] OJ L 172/79 recital 16.

[135] See by analogy Directive 2019/790 (n 72) Article 17(4).

[136] See e.g. Castets-Renardt (n 129).

[137] The White House, 'Fact Sheet: President Donald J. Trump Issues Directive to Prevent the Unfair Exploitation of American Innovation' (*The White House*, 21 February 2025) <https://www.whitehouse.gov/fact-sheets/2025/02/fact-sheet-president-donald-j-trump-issues-directive-to-prevent-the-unfair-exploitation-of-american-innovation/> accessed 1 September 2025.

[138] Dean Jackson and Berin Szóka, 'The Far Right's War on Content Moderation Comes to Europe | TechPolicy.Press' (*Tech Policy Press*, 11 February 2025) <https://techpolicy.press/the-far-rights-war-on-content-moderation-comes-to-europe> accessed 1 September 2025.

[139] Daniel Hickey et al, 'X under Musk's Leadership: Substantial Hate and No Reduction in Inauthentic Activity' (2025) 20(2) PLOS ONE e0313293.

expression posed by over-moderation. The Commission and the CJEU, through case law and subsequent codification in the DSA have arguably opted for a broad scope for intermediary liability exemption. Nevertheless, narrowing the interpretation of the intermediary liability exemption in some cases can be justified to inspire better moderation efforts by intermediary service providers to provide counterweight to the 'moderation withdrawal'.

3.5 FREEDOM OF EXPRESSION IS NO PRIMA FACIE OBSTACLE TO A MORE NARROW INTERPRETATION

A main point of critique against restricting intermediary liability exemption is that it would interfere with freedom of expression, since strict liability may lead to over-removal. However, the ECtHR leaves considerable room for intermediary liability in its case law, suggesting that freedom of expression does not stand in the way of a more narrow interpretation of the liability exemption.

In its case law, the ECtHR balances rights of individuals affected by defamation or hate speech against the right to freedom of expression of hosting providers. In that balancing act it does not consider the liability exemption of Articles 14 ECD or 6 DSA[140] – nor does it have to.[141] For example, in *Delfi v Estonia,* the ECtHR found that holding a newspaper liable for hate speech posted by anonymous users was not in violation of the right to freedom of expression of Article 10 ECHR, without considering that such a newspaper would enjoy liability exemption.[142] In *MTE v Hungary,* the ECtHR considered holding a Hungarian association liable for hosting 'false and offensive' comments to interfere with the freedom of expression, since the notion of liability applied by the national courts did not allow for a balancing of interests between competing rights.[143] It explicitly did not consider the liability exemption.[144] In its latest seminal judgment on the matter, *Sanchez v France,* the ECtHR confirms the line of *Delfi,* and even extends it to apply to a politician who was held criminally liable for not removing hateful comments by third parties on his Facebook page.[145] In this case too, the Court did not rely on the liability exemption following the national court's assessment on that matter,[146] but also emphasises that 'to exempt

[140] *Delfi v Estonia* (n 6) para 127; Oreste Pollicino, 'European Judicial Dialogue and the Protection of Fundamental Rights in the New Digital Environment: An Attempt at Emancipation and Reconciliation' in Sonia Morano-Foadi and Lucy Vickers (eds), *Fundamental Rights in the EU: A Matter for Two Courts* (Bloomsbury Publishing 2015) 108; Marta Maroni, 'The Liability of Internet Intermediaries and the European Court of Human Rights' in Bilyana Petkova and Tuomas Ojanen (eds), *Fundamental Rights Protection Online* (Edward Elgar Publishing 2020) 268.

[141] Martin Husovec et al, 'Grand confusion after *Sanchez v. France*: Seven reasons for concern about Strasbourg jurisprudence on intermediaries' (2024) 31(3) Maastricht Journal of European and Comparative Law 385. Cf. Michael FitzGerald, 'Not hollowed by a Delphic frenzy: European intermediary liability from the perspective of a bad man: A response to Martin Husovec et al.' (2025) 32(1) Maastricht Journal of European and Comparative Law 47.

[142] *Delfi v Estonia* (n 6) paras 160-161. Lisl Brunner, 'The Liability of an Online Intermediary for Third Party Content: The Watchdog Becomes the Monitor: Intermediary Liability after *Delfi v Estonia*' (2016) 16(1) Human Rights Law Review 163.

[143] *MTE and Index.hu v Hungary* (n 29) para 89.

[144] ibid para 51; it accepted the national court's reasoning that MTE did not qualify as a hosting provider because it did not provide e-commerce services.

[145] *Sanchez v France* (n 6) para 209.

[146] ibid paras 137-139.

producers (as a specific subclass under French civil law) from all liability might facilitate or encourage abuse and misuse, including hate speech and calls to violence, but also manipulation, lies and disinformation'.[147]

The argument here is that freedom of expression does not need to stand in the way of a more narrow interpretation of the liability exemption. When interpreting the DSA in light of the Charter[148] – which forms a guiding document following recital 153[149] – the case law of the ECtHR leaves room for a narrower interpretation of liability exemption without interfering with freedom of expression. This narrow interpretation would emphasise the need for due diligence by hosting providers. Of course, the potential risks to freedom of expression of stricter liability need to be weighed against the benefits of that liability, and much depends on the factual assessment by national courts of whether the internet intermediary qualifies as a hosting provider. The ECtHR has developed a line of case law that explicitly acknowledges the possibility for establishing liability for internet intermediaries, and the freedom of expression does not necessarily need to stand in the way of stricter liability exemption.

This section has provided arguments for a narrower interpretation of intermediary liability exemption. These are rooted in the conviction that, since the role of hosting providers in society has increased significantly since the year 2000 and their capacities have evolved correspondingly, it is fair to come to a narrower interpretation of the liability exemption. Of course, this narrow interpretation needs to be grounded in law. The next section explores avenues in the DSA that allow for a narrower interpretation of the intermediary liability exemption.

4 HOW DOES THE DSA ALLOW FOR RETHINKING THE INTERMEDIARY LIABILITY EXEMPTION?

Section 3 has provided arguments for why a narrow interpretation of the hosting liability exemption may be desirable and possible from a fundamental rights perspective. This Section explores which provisions in the DSA can be used to that argumentation. The DSA can allow applying the liability exemption more narrowly. The purpose of the narrow interpretation is to exclude bad faith actors from the liability exemption. An actor can be considered in bad faith when it is generally incompliant with the DSA's due diligence norms, or undiligent in its handling of notices to avoid awareness of illegal content. Although Section 2.2 has explained why due diligence obligations are separated from liability questions, the threshold for intermediary liability exemption still introduces a level of diligence expected from intermediaries to determine whether they are a hosting provider that was not aware of illegal content.

This raises a question: what happens when an undiligent economic operator is presented with facts or circumstances that would have created awareness of illegal content within the framework of the DSA had they been diligent? This Section argues that an undiligent economic operator may be excluded from the liability exemption for two

[147] *Sanchez v France* (n 6) para 185.
[148] Which must be interpreted in light of the European Court of Human Rights case law following Article 52(3) of the Charter of Fundamental Rights of the European Union.
[149] Digital Services Act (n 4) recital 153.

reasons: (i) intermediary services that structurally infringe on Articles 16(1) and 23(1) DSA do not qualify as a neutral hosting provider in the sense of Article 6(1) DSA, and/or (ii) the undiligent hosting provider has failed to remove content of which the diligent provider ought to have been aware in light of Article 16(6) DSA and sectoral due diligence norms.

4.1 AN UNDILIGENT INTERMEDIARY CAN BE EXCLUDED FROM QUALIFYING AS A NEUTRAL HOSTING PROVIDER UNDER ARTICLE 6(1)

A first line of argumentation is that an undiligent intermediary service provider should not qualify as a passive, neutral hosting provider. The requirements for a hosting provider are that internet intermediary services provide their services neutrally, by mere technical and automatic processing of information.[150] To be excluded from this category, a hosting provider either has active knowledge over content, or has control over the content shared. This threshold is not met easily: as mentioned in subsection 2.1[a], platforms may structure, recommend, and index content without being excluded from being a hosting provider. However, as demonstrated in subsection 2.1[b], the hosting provider may not deliberately facilitate dissemination of illegal content: hosting providers are excluded from liability exemption when they have openly expressed the intention to facilitate illegal content.[151] This is also reflected in recital 20 of the DSA: in instances where the intermediary service 'deliberately collaborates' with a user they are not neutral and therefore should not benefit from the liability exemption. In line with the case law cited above, this is the case when intermediary service providers make explicit that their purpose is to facilitate illegal activities.

However, the threshold of open expression of intention to facilitate illegal content is not insignificant, and is therefore unlikely to exclude many 'bad faith' hosting providers, even though that could be desirable from the perspective of combatting illegal content and providing remedies to aggrieved parties. Holznagel notes that the requirements of neutrality and passivity, the 'knowledge-or-control' test, does not necessarily exclude providers that are structurally prone to hosting illegal content ('*strukturell gefahrgeneigter Provider*') from liability exemption.[152] He mentions Darknet platforms and platforms with limited protection for revenge porn as examples.[153] These types of hosting providers may be passive, neutral and not control the illegal content hosted on their platform, and thus qualify as a hosting provider under Article 6 DSA, exempting them from liability if they remove content expeditiously after a notice.[154] At the same time, they are prone to hosting illegal content. This protection may therefore be overly broad: although platforms cannot be held liable based on general

---

[150] Digital Services Act (n 4) recital 18, see subsection 2.1[a].
[151] See to that effect: Case C-527/15 *Stichting Brein v Filmspeler* EU:C:2017:300; Case C-610/15 *Stichting Brein v Ziggo & XS4All,* EU:C:2017:456; Opinion of AG Saugmandsgaard Øe in *YouTube/Cyando* (n 39) paras 120, 129 and 191.
[152] Again, with the exception of those that openly facilitate illegal content, in this case *Filmspeler* and *ThePirateBay*; Daniel Holznagel, 'Nach dem EuGH-Urteil in Sachen YouTube/Cyando: Fast alles geklärt zur Host-Provider-Haftung?' (2021) 37(9) Computer und Recht 603, 605.
[153] Daniel Holznagel, 'Chapter II Des Vorschlags Der EU-Kommission Für Einen Digital Services Act — Versteckte Weichenstellungen Und Ausstehende Reparaturen Bei Den Regelungen Zu Privilegierung, Haftung & Herkunftslandprinzip Für Provider Und Online-Plattformen' (2021) 37(2) Computer und Recht 123, 124.
[154] Digital Services Act (n 4) Article 6(1)(b).

knowledge that they host illegal content under CJEU case law, it seems overly protective to offer liability exemption to platforms who have such general knowledge and act non-diligently in the design of their services with respect to illegal content. An exemption from liability may not encourage any moderation efforts, as Buiten et al have stipulated, and may even be conducive to sinister business-models that seek to monetise illegal content.[155]

A-G Saugmandsgaard Øe concluded – albeit in a footnote – in 2020 that the liability exemption is only intended for hosting providers acting in good faith.[156] This consideration has not been adopted explicitly in decisions by the CJEU, or in the DSA.[157] Holznagel wrote in 2021 that excluding bad faith hosting providers as 'non-neutral' would require a formal alteration of the standards for being a hosting provider.[158] However, the distinction between passive and active has diminished somewhat in the DSA; the DSA explicitly allows platforms to take an active stance toward content without losing their liability exemption, for example by indexing or filtering content.[159] An answer to the impossibility regarding the exclusion of bad faith actors would be to exclude structurally prone-to-illegal-content platforms from qualifying as a neutral[160] hosting provider, and therefore excluding them from the liability exemption.

What does it mean to be a non-neutral hosting provider? Under the ECD, being neutral – aside from the practical implications of providing the service without taking any editorial responsibility or control over the content – was generally interpreted as abiding by takedown requests and taking some content moderation measures, but left room for interpretation on where the borders of neutrality are.[161] It can be argued that under the DSA, some aspects are formally required from neutral hosting providers in order to maintain their liability exemption: Article 9 DSA provides a clear avenue establishing clear takedown requests by administrative entities, which, by repeated refusal or non-compliance, could lead to the conclusion that the hosting provider is not neutral. Similarly, Article 16(6) requires hosting providers to engage in good faith with notices submitted through notice-and-action mechanisms. Equally, Article 23, on abusive users, requires that hosting providers act in good faith in maintaining their user-base, and exclude abusive recipients from their service. If a significant part of the user base of a platform is abusive, this could exclude the hosting provider from neutrality. Non-compliance could preclude hosting provides from acting in a 'neutral' capacity, and therefore exclude them from the liability exemption of Article 6. The subsections 4.1[a] and 4.1[b] explain why Articles 16 and 23 provide legal instruments that enable the exclusion of intermediary service providers that are structurally prone to hosting illegal content or generally act in bad faith from the liability exemption.

---

155 Buiten, de Streel, and Peitz (n 121) 150–151.
156 Opinion of AG Saugmandsgaard Øe in *YouTube/Cyando* (n 39) fn 187.
157 Although Article 7 DSA on the Good Samaritan provision could be read as rewarding good faith economic operators with liability exemption, even if they are aware of illegal content.
158 Holznagel, 'Nach dem EuGH-Urteil in Sachen YouTube/Cyando' (n 152) 606.
159 Digital Services Act (n 4) recital 22.
160 Focussing on neutrality rather than passivity is in line with CJEU case law, e.g. Opinion of AG Jääskinen in *L'Oreal v eBay* (n 48) paras 138-146; see also van Hoboken et al (n 37) 31-32.
161 Wilman, 'The EU's System of Knowledge-Based Liability for Hosting Services Providers in Respect of Illegal User Content – Between the e-Commerce Directive and the Digital Services Act' (n 16) 321.

4.1[a] Dysfunctional or no notice-and-action mechanisms under Article 16

As noted in Section 3.1, notice-and-action mechanisms are an important aspect of the intermediary liability exemption framework. However, before the DSA, there was no general legal requirement for intermediary services to provide such a mechanism.[162] Varying national implementations, and some sectoral (co)-regulations recommended,[163] or indeed required,[164] intermediary services providers to provide such mechanisms. Article 16 adds to this paradigm with a horizontal requirement for hosting providers to provide user-friendly and easily-accessible mechanisms that allows anyone to notify them of illegal content.[165] Remedies for users for non-compliance with this article would, in line with the framework outlined in Section 2.4, fall under Article 54 DSA on damages.

However, conceptualising the hosting provider as a neutral, good faith intermediary, it can be argued that failing to provide users with a notice-and-action mechanism under Article 16(1) DSA excludes intermediary service providers from qualifying as a hosting provider, and thus from liability exemption. Holznagel underscores this argumentation, noting that missing notice-and-action mechanisms could be an indicator for an 'active role' due to creating a structural risk for illegal content.[166] The reasoning for this is that notice-and-action is the only available remedy for users in the liability exemption framework, with the exception of overly burdensome and time-consuming procedures to acquire injunctions in national courts, which still may be an ineffective remedy due to the speed at which illegal content spreads on the internet.[167] If intermediary service providers do not present users with the possibility of 'creating' awareness of illegal content – after all, a notice under Article 16 is seen as creating such awareness[168] – they might not be able to be held liable. Lacking a notice-and-action mechanism should be seen as bad-faith design of the hosting service; by being negligent in respect of Article 16, the hosting provider ensures that liability exemption of Article 6(1)(a) would always be available. This cannot be the intention of the EU regulator. Not facilitating a notice-and-action mechanism must therefore lead to a potential exclusion from the intermediary liability exemption.

Following this argumentation, the question arises whether the degree of non-compliance with Article 16 should factor into the assessment whether the hosting provider takes an active approach. Notice-and-action mechanisms, after all, can take different

---

[162] Pieter Wolters and Raphaël Gellert, 'Towards a Better Notice and Action Mechanism in the DSA' (2023) 14(3) Journal of Intellectual Property, Information Technology and Electronic Commerce Law 403; MZ van Drunen, 'The Post-Editorial Control Era: How EU Media Law Matches Platforms' Organisational Control with Cooperative Responsibility' (2020) 12(2) Journal of Media Law 166, 177. Although some argue that the ECD indirectly requires platforms to adopt notice and action mechanisms, see Aleksandra Kuczerawy, Kuczerawy, 'From "Notice and Takedown" to "Notice and Stay Down"' (n 62).

[163] E.g. European Commission, 'Code of Conduct on Countering Illegal Hate Speech Online' <https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en> accessed 1 September 2025; now updated to the Code of conduct on Countering Illegal Hate Speech Online + (n 61), adopted under Article 45 DSA.

[164] Regulation 2021/784 (n 134) Article 10; Directive 2019/790 (n 72) Article 17(9).

[165] Digital Services Act (n 4) Article 16(1); Article 3(h).

[166] Holznagel, 'Chapter II Des Vorschlags Der EU-Kommission Für Einen Digital Services Act' (n 153) 126.

[167] That is not to say that users cannot attempt to request takedown outside of the mechanisms of Article 16; see recently Kammergericht Berlin, 25 August 2025, 10 W 70/25.

[168] Digital Services Act (n 4) Article 16(3).

forms,[169] and compliance with the requirements of Article 16 is varying across hosting providers.[170] This has to be assessed on a case-by-case basis, in line with the spectrum of neutral activities mentioned in subsection 2.1[a]. It is disproportional to the ratio of Article 6 to exclude intermediary service providers from liability exemption for being slightly difficult to use; however, if the notice-and-action mechanism is absent, or is designed in such a way that users are unable to meet the criteria of submitting an adequately substantiated notice by using these mechanisms, it could be fair to exclude them from being labelled as a neutral hosting provider. For example, if a platform does not facilitate an explanation of the illegality of a notice, it is possible that this precludes an adequately substantiated notice, which requires an explanation of the legal ground under which the content is illegal and an explanation of why the content is illegal.[171] Being unable to explain the illegality in sufficient detail would leave the user unable to create awareness under CJEU case law.

A functioning-notice-and-action system is a *conditio sine qua non* for the liability exemption framework in the DSA. Rewarding intermediary service providers that fail to contribute to that system with liability exemption is unfair, especially in light of the many (co-)regulatory instruments requiring such a mechanism. The proportionality of excluding hosting providers from the liability exemption is ensured by the fact that Article 16(1) poses form-free requirements, and hosting providers have the freedom to comply in a way that suits their service best.[172] The requirements therefore do not significantly impede on the freedom of enterprise of hosting providers, nor do they pose excessive burdens.[173] It is therefore not unfair that non-compliance with Article 16 could lead to the hosting provider being excluded from the liability exemption of Article 6 DSA, by excluding such providers from qualifying as a neutral hosting provider, especially in light of the strict requirements posed on notices to create specific knowledge or awareness of illegal content.[174]

4.1[b] Misuse of services under Article 23(1)

Article 23(1) is a due diligence obligation that requires online platforms to suspend users that frequently provide manifestly illegal content.[175] It requires online platforms (as a subcategory of hosting providers)[176] to be aware of users that misuse their services and exclude them. This prevents online platforms from being populated with illegal content by 'repeat offenders'. The argument in this subsection is that structurally disregarding abusive users that frequently post illegal content online may exclude an intermediary service provider from qualifying as a neutral hosting provider. The CJEU acknowledged that repeat infringers could

[169] Kate Crawford and Tarleton Gillespie, 'What Is a Flag for? Social Media Reporting Tools and the Vocabulary of Complaint' (2016) 18(3) New Media & Society 410.
[170] Sekwenz, Wagner, and Parkin (n 118).
[171] See further examples: Sekwenz, Wagner, and Parkin (n 118).
[172] Hofmann and Raue (n 18) 328.
[173] Cf. Wolters and Gellert (n 162) 408; Christophe Geiger, Giancarlo Frosio, and Elena Izyumenko, 'Intermediary Liability and Fundamental Rights' in Giancarlo Frosio (ed), *Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020).
[174] Digital Services Act (n 4) recital 22: '[…] through notices submitted to it by individuals or entities in accordance with this Regulation in so far as such notices are sufficiently precise and adequately substantiated to allow a diligent economic operator to reasonably identify, assess, and where appropriate, act against the allegedly illegal content'. Also: *YouTube/Cyando* (n 6) para 116.
[175] Digital Services Act (n 4) Article 23(1).
[176] ibid Article 3(i).

require an additional level of diligence by the hosting provider. In *L'Oreal,* the Court decided that hosting providers may be required to suspend users who repeatedly post copyright infringing content to prevent future infringements.[177] Hofmann underscores this argument, noting that infringing on the duty of care laid down in Article 23 can lead to the assumption of an active role for the platform provider.[178]

The *ratio* behind the exclusion from the liability exemption is that structural non-compliance with Article 23 is an indication of a bad faith approach to content moderation. The indication that non-compliance represents bad faith is informed the fact that Article 23 in itself represents high thresholds regarding the frequency and the manifest illegality of the content disseminated, meaning that only a negligent hosting provider could have missed an abusive user. The frequency necessary to trigger Article 23(1) is dependent on the requirements laid down in Article 23(3): the absolute volume of illegal content provided, and the proportion of the illegal content compared to legal content.[179] The manifest illegality of the content is dependent on whether a layperson would see the content as evidently illegal.[180] It could be argued that the nature of the manifestly illegal content should be a factor in determining compliance with Article 23: while a layperson may be able to detect fake Birkenstocks as trademark infringement, a platforms failure to block accounts spreading CAM may be more damning under Article 23(1) if the requirement refers to 'manifestly illegal content'. Similarly, one could argue that frequency and manifest illegality can be corresponding factors, meaning that a high frequency of less evidently illegal content could still trigger Article 23(1), as well as a comparatively lower frequency of very evidently illegal content, such as CAM. Since excluding online providers from the liability exemption is a significant step, the proportionality of the exclusion needs to be weighed against the degree of non-compliance with article; it would be disproportional to exclude a platform with over a billion users due to failing to suspend services for one abusive user. Non-compliance with Article 23 therefore needs to be structural. This needs to be assessed on a case-by-case basis and can depend *inter alia* on the nature of the illegality prevalent on the platform, the proportion of users that can be labelled as abusive under Article 23, and the measures taken to combat such abuse.

Aside from not qualifying as a neutral hosting provider, it could be argued that, even if the online platform was unaware of illegal content posted by such a 'repeat offender', it should have been due to the requirements of Article 23(1). This relates to the point made in the next subsection in which provisions in the DSA can be used to lower the threshold for when a hosting provider is deemed aware of illegal content. In the case of abusive users, knowledge of that illegal content is then construed by the explicit expectations of the due diligence provision in Article 23(1). Again, this provision needs to be applied proportionally to the impact that excluding hosting providers from the liability exemption would have. The bar for being an abusive user in Article 23(1) is therefore not met easily, Raue argues, and

[177] *L'Oreal v eBay* (n 6) para 141.
[178] Hofmann and Raue (n 18) 163.
[179] Digital Services Act (n 4) Article 23(3).
[180] ibid recital 63. This seemingly constitutes a stricter barrier than the illegality that needs to be indicated by users in a notice under article 16, as found in: *YouTube/Cyando* (n 6) para 116: 'sufficient information to enable the operator of that platform to satisfy itself, without a detailed legal examination, that that communication is illegal and that removing that content is compatible with freedom of expression'.

only with respect to the interests of all parties involved.[181] This may limit the instances where non-compliance with Article 23(1) leads to exclusion from intermediary liability exemption in practice. However, the high threshold of applying Article 23(1) underscores the severity of the non-compliance by the hosting provider, and it supports the notion that it is proportional that, when a platform provider is taking a bad-faith approach to content moderation and fails to take action in Article 23(1) situations, they no longer qualify as a neutral hosting provider.

4.2 THE THRESHOLD FOR AWARENESS IN DILIGENT ECONOMIC OPERATORS IS LOWER

The previous section has argued that non-compliance with Articles 16 and 23 DSA may lead to exclusion from qualifying as a neutral hosting provider; those actors can therefore not rely on the liability exemption by default. This section moves one step further: if an intermediary service provider qualifies as a hosting provider, provisions in the DSA and sectoral regulation can lower the threshold of awareness of illegal content with diligent economic operator under Article 6(1)(a)DSA in factual assessments. If the hosting provider does not act expeditiously after becoming aware of illegal content, they are excluded from the liability exemption following article 6(1)(b).[182]

The expectation of diligence in relation to awareness of illegal content is introduced in subsection 2.1[b]: a hosting provider may not rely on the liability exemption if they are aware of facts or circumstances that would have led a diligent economic operator to identify the illegality. This criterion, to some extent, creates an expectation of diligence from hosting providers. This diligence can be interpreted as a duty of care. The CJEU created some room for this interpretation in *L'Oréal,* which was not completely resolved in *YouTube,* especially in light of the tension that a duty of care would bring with the prohibition on general monitoring obligations. In *L'Oréal,* the CJEU found that an imprecise notice must still be taken into account by a diligent operator.[183] *YouTube* clarifies that in those instances the notice must still contain sufficient information to remove the content without a detailed legal examination.[184] The degree to which this requires a duty of care was never fully resolved in case law, but *Youtube* indicates that the duty of care is not broad. However, the DSA introduces a number of provisions that can be used to define the threshold for when a hosting provider is deemed aware of illegal content in line with that duty of care.

This section proposes that developments in the DSA and sectoral regulation arguably lower the factual threshold for establishing awareness of illegal content on a factual level compared to the ECD, for example in cases where a notice is insufficiently precise, or even absent. This is supported by two arguments: (a) Article 16(6) explicitly requires better diligence on notices on ongoing infringement; (b) duties of care established in sectoral regulation reduce the amount of information required to raise knowledge or awareness. These two arguments are supported by the general notion that, since content moderation mechanisms have become incrementally more sophisticated than they were under the ECD

[181] Hofmann and Raue (n 18) 472.
[182] Digital Services Act (n 4) Article 6(1)(b).
[183] *L'Oreal v eBay* (n 6) para 122.
[184] *YouTube/Cyando* (n 6) para 116.

(see Section 3.3), it is not unreasonable to expect that hosting providers have awareness of illegal content sooner than they would have 25 years ago.

4.2[a] Article 16(6) DSA requires more diligence in assessing notices

As part of the newly formalised notice-and-action framework, Article 16(6) DSA stipulates that decisions on the information in any notices received through the mechanisms of Article 16(1) must be taken in a timely, diligent, non-arbitrary and objective manner.[185] This is predominantly a codification of jurisprudence, and outlines requirements that can be used to fill in a 'duty of care' for hosting providers on notices. It is important to note that these principles are a matter of procedure, not outcome. Article 16(6) does not entitle a user to a correct decision, just to a timely, non-arbitrary, objective, and diligent decision.[186] Such decisions may also be rendered using automatic means.[187] Aside from the timeliness requirement, which is fluid and needs to be established on a case-by-case basis, notices need to be examined in a diligent, non-arbitrary, and objective manner. While non-arbitrariness and objectivity are requirements that are part of the proceduralisation of content moderation,[188] the argument of this subsection is that the requirement of diligence of Article 16(6) may lower the threshold for awareness of illegal content, as a diligent economic operator can be deemed aware of illegal content sooner.

The next question is: how diligent does a notice need to be examined? Generally, the level of diligence required is relatively low, Holznagel argues, in light of the finding in *Youtube* that illegality needs to be established without a detailed examination of the notice.[189] However, providers could be assumed to have gained knowledge if the provider 'negligently ignores evidence for a violation'.[190] On a practical level this includes information included in a notice by users, but also existing and easily accessible knowledge, such as the context of the alleged violation, the history of the reporter, and the history of the uploader.

In line with the argumentation in Section 3.3: it is not inconceivable that existing and easily accessible knowledge is more present than it was 20 years ago; it could therefore be argued that factually, negligently ignoring evidence of a violation is likely to happen more frequently. The DSA also creates a number of examples that facilitate access to knowledge outside of the information contained in the notice. For example, trusted flagger status, as part of the history of the reporter, under Article 22 can be a relevant factor.[191] On the history of the uploader: if a user frequently uploads manifestly illegal content, the online platform is expected to be aware of that content under Article 23. As argued in the previous Section,

[185] Digital Services Act (n 4) Article 16(6).
[186] Wolters and Gellert (n 162) 415.
[187] Explicitly: Article 16(6): '[…] *Where they use automated means for that processing or decision-making*, they shall include information on such use in the notification referred to in paragraph 5' (emphasis added).
[188] Interestingly they assume that the hosting provider is a neutral actor that has no opinions or preferences of its own. However, the European Court of Human Rights acknowledged to some extent in *Google v Russia* that hosting providers can have their own freedom of expression: see *Google LLC and others v Russia,* App no 37027/22 (EctHR, 8 July 2025) para 91.
[189] Daniel Holznagel, 'How to Apply the Notice and Action Requirements under Art. 16(6) Sentence 1 DSA – Which Action Actually?' (2024) 25(6) Computer Law Review International 172, 177.
[190] ibid.
[191] Digital Services Act (n 4) Article 22(1). Arguably, the opposite is true for users that frequently abuse the notice-and-action mechanism. The online platform is expected to suspend their flagging mechanisms under Article 23(2).

knowledge on illegal content can be construed in such situations based on the explicit due diligence obligation for the online platform. Previous knowledge on the nature of the infringing content could be established through earlier notices under Article 16, appeals under Article 20,[192] or potentially earlier decisions regarding identical or similar content in the out-of-court dispute settlement framework of Article 21.[193] It is possible that the same content is reported multiple times by the same reporter: the DSA does not prevent *ne bis in idem* with regards to notices on illegal content. This causes a hosting provider to have some prior knowledge on a specific infringement.

An additional question is whether Article 16(6) requires diligence only with regards to the specific information contained in the notice, or also requires reflection on similar or identical illegal content, thus creating a potential takedown obligation for more than the content exactly indicated in the notice. This tension was touched upon under subsection 2.1[c] as notice-and-staydown.[194] Holznagel argues that this is not the intention of the notice-and-action framework of Article 16(6): the relating recitals and legislative process do not support it.[195] However, if identical or similar content is understood as an ongoing infringement, as opposed to separate information that was not included in the original notice, then a diligent hosting provider might be expected to address such content.

The understanding of ongoing infringement is in line with A-G Jääskinen's conclusion in *L'Oreal*, in which he illustrates that:

> if A has been discovered infringing trade mark X by listing an offer on the electronic marketplace in September, I would not exclude that the marketplace operator could be considered having actual knowledge of information, activity, facts or circumstance if A uploads a new offer of the same or similar goods under trade mark X in October. In such circumstances it would be more natural to speak about the same continuous infringement than two separate infringements. I recall that Article 14(1)(a) mentions 'activity' as one object of actual knowledge. An ongoing activity covers past, present and future.[196]

Jääskinen's argumentation includes a strong temporal dimension (i.e. the time from September to October). Whether this applies to a wider timeframe (e.g. from September to January) needs to be assessed on a case-by-case basis. It is difficult to speak of ongoing infringement if this timeline was 5 years instead of a mere month; such would be overly burdensome to the hosting provider, and create a tension with the prohibition on general monitoring obligations. However, qualifying similar and identical content as ongoing infringement may require a hosting provider to remove such illegal content as well as part of the diligence required under Article 16(6). This expected diligence can create circumstances in which a platform is deemed to be aware of illegal content, even though a notice referring the content may not have been specific enough to raise knowledge on illegal content. This interpretation of Article 16(6) would be in line with the CJEU's decision in *Glawischnig-Piesczek*, in which an effective remedy could only be achieved through granting an injunction

[192] ibid Article 20.
[193] ibid Article 21.
[194] *Eva Glawischnig-Piesczek v Facebook* (n 67) para 41.
[195] Holznagel, 'How to Apply the Notice and Action Requirements' (n 189) 178.
[196] Opinion of AG Jääskinen in *L'Oreal v eBay* (n 48) para 167.

for 'similar' content. If a hosting provider fails to address content that *should* have been identified through diligent assessment of the notice, it could be excluded from Article 6(1). Of course, the level of diligence in this case needs to be balanced against the general monitoring prohibition, but *Glawischnig-Piesczek* opens the door to a more expansive reading of diligence.

4.2[b] Duties of care established in sectoral regulation and the DSA raise the bar for the diligent economic operator

The DSA is the horizontal cornerstone of the digital *acquis,* but succeeds a number of sectoral (co-)regulations that establish duties of care for hosting providers (or a sector-specific subset thereof). Some sectoral regulation exists outside of the scope of DSA liability exemption, such as the CDSM.[197] However, other regulatory and co-regulatory instruments, such as the amendments to the Audiovisual Media Services Directive (AVMSD),[198] the Regulation preventing the dissemination of terrorist content online (TERREG)[199] and several codes of conduct,[200] introduce explicit due diligence obligations for hosting providers or their corresponding sector-specific subset. This subsection argues that the level of diligence of economic operators required by Article 6(1) DSA needs to be interpreted in line with duties of care that are imposed on hosting providers in the varying sectoral regulations. In cases where information is not clearly available through the notice submitted because it is incomplete, duties of care required in sectoral (co-)regulation may lower the threshold of information contained in the notice for the platform to still make an assessment on the legality of the content.

One example of sectoral regulation requiring additional due diligence from hosting providers is the amended AVMSD. The DSA applies without prejudice to this Directive.[201] The AVMSD applies to media service providers – a categorisation distinct from the categorisations made in the DSA. Particularly relevant are 'video-sharing platform services', a subset of media service providers, are essentially platforms that allow the dissemination of user-generated videos to the general public.[202] This affordance is common for online platforms under the DSA; most VLOPs and online platforms are therefore required to comply with the AVMSD parallel to the DSA.[203] Under Article 28b(1) AVMSD,

[197] Digital Services Act (n 4) recital 11; Directive 2019/790 (n 72).
[198] Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities [2018] OJ L 303/69.
[199] Regulation 2021/784 (n 134).
[200] European Commission, 'Code of Conduct on Disinformation' (13 February 2025) <https://digital-strategy.ec.europa.eu/en/library/code-conduct-disinformation> accessed 1 September 2025; Code of conduct on Countering Illegal Hate Speech Online + (n 61).
[201] Digital Services Act (n 4) recital 10. Interestingly Article 28b applies without prejudice to Articles 12 to 15 of the ECD, which leaves the relation between the DSA and the AMVSD unclear.
[202] Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) [2010] OJ L95/1 Article 1(aa).
[203] Sally Broughton Micova and Ľuboš Kukliš, 'Responsibilities of Video-Sharing Platforms and Their Users' in Heritiana Ranaivoson, Sally Broughton Micova, and Tim Raats (eds), *European Audiovisual Policy in Transition* (Routledge 2023) 88.

video-sharing platforms are expected to adopt appropriate measures to protect minors from commercial content that impairs their development, and the general public from commercial content containing violence, hate speech, terrorist content, or CAM.[204] The appropriateness of such measures is determined in light of the nature of the content, the harm it may cause, and the interests of the group protected and the public at large.[205] This generally means that larger platforms will need to take more appropriate measures against such content than smaller platforms.[206] Platforms must include and apply such measures in their terms and conditions – underlining that some level of diligence is required.[207] This is safeguarded by establishing a notice-and-action mechanism and dispute resolution procedures.[208] Appropriate measures are bound by the prohibition of general monitoring obligations of Article 8, and can therefore not involve preventive filtering of content.[209] Nevertheless, Ullrich underlines that some 'morally and technically founded duties of care' would be appropriate in the context of the AVMSD.[210] This gap is, since his writing, partially filled by the due diligence framework of the DSA, but the notion that the requirements of the AVMSD create an extra duty of care for platforms still stands after the DSA's adoption. A more diligent investigation into notices regarding CAM, hate speech, or terrorist content is therefore required from video-sharing platform services by reading the AVMSD in conjunction with the DSA.

Another example of sectoral regulation introducing additional requirements for hosting providers is TERREG. TERREG applies parallel to the DSA and the AVMSD.[211] It applies to hosting service providers, a definition found in the Information Society Services Directive that largely mirrors the definition of hosting provider in the DSA.[212] The Regulation tackles the dissemination of terrorist content online by laying down duties of care for hosting providers.[213] When a hosting provider is confronted with terrorist content in the last 12 months – which is virtually all large online platforms – they are required to take extra measures.[214] These measures include addressing removal orders within one(!) hour, flagging channels for EUROPOL and other competent authorities, notice and action mechanisms, and taking proactive measures to combat illegal content.[215] Several researchers have criticised this Regulation for introducing a pro-active duty of care that would contravene

[204] Directive 2010/13/EU (n 202) Article 28(b).
[205] ibid Article 28b(3).
[206] Pietro Dunn, 'Online Hate Speech and Intermediary Liability in the Age of Algorithmic Content Moderation' (PhD thesis, University of Bologna 2024) 90–91.
[207] Directive 2010/13/EU (n 202) Article 28b(3)(a)-(b); also Giovanni De Gregorio, 'Expressions on Platforms' (2018) 2(3) European Competition and Regulatory Law Review 203, 212–213.
[208] Directive 2010/13/EU (n 202) Article 28b(3)(d)-(i).
[209] ibid; *mutatis mutandis*: 'Those measures shall not lead to any ex-ante control measures or upload-filtering of content which do not comply with Article 15 of Directive 2000/31/EC'.
[210] Carsten Ullrich, 'Standards for Duty of Care: Debating Intermediary Liability from a Sectoral Perspective' (2017) 8(2) Journal of Intellectual Property, Information Technology and Electronic Commerce Law 111, 118–119.
[211] Regulation 2021/784 (n 134) Article 1(5); Digital Services Act (n 4) recital 10.
[212] Regulation 2021/784 (n 134) Article 2(1); Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification) [2015] , art. 1(b).
[213] Regulation 2021/784 (n 134) Article 1(1)(a).
[214] Regulation 2021/784 (n 134) Article 4(4).
[215] ibid Article 4(1).

Article 8 DSA.[216] Platforms would be expected to use automated means to filter illegal content, which arguably presents risks for freedom of expression, certainly in light of the broad definition of terrorist content in the Regulation.[217] This critique is generally well-founded; however, with regards to liability exemption – which van Hoboken argues is partly undermined by the Regulation – it could be argued that platforms are expected to be more diligent when users submit notices on terrorist content, both regarding the required expedience in taking action and the degree to which platforms are expected to take down identical and similar content. Because the platform is required in sectoral regulation to be more diligent, the threshold for when a platform is aware of that illegal content is lower when a user reports terrorist content, even when that notice is not precise, or if it did not remove content identical to a previous notice.

Sectoral codes of conduct can also add requirements to content moderation practices, in particular with regards to illegal hate speech and disinformation.[218] The DSA explicitly formalises Codes of Conduct as part of the DSA framework.[219] Codes of Conduct are traditionally voluntary, multistakeholder efforts that shape policy and facilitate participation in content moderation.[220] Although the DSA emphasises their voluntary nature,[221] it has been theorised that there is significant pressure to adhere to the standards of such codes.[222] This is underscored by recital 104 stressing that

> […] the refusal without proper explanations by a provider of an online platform or of an online search engine of the Commission's invitation to participate in the application of such a code of conduct could be taken into account, where relevant, when determining whether the online platform or the online search engine has infringed the obligations laid down by this Regulation.[223]

Generally, complying with codes of conduct will make hosting providers more aware of illegal content on a practical level, for example by engaging with trusted flaggers and fact-

---

[216] Inter alia Alexandre De Streel, 'Online Platforms' Moderation of Illegal Content Online' (European Parliament 2020, PE 652.718), 25–26 <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652718/IPOL_STU(2020)652718_EN.pdf> accessed 1 September 2025; Joris van Hoboken, 'The Proposed EU Terrorism Content Regulation: Analysis and Recommendations with Respect to Freedom of Expression Implications' (Transatlantic Working Group on Content Moderation Online and Freedom of Expression 2019), 7 <https://pure.uva.nl/ws/files/46500757/46218669.pdf> accessed 1 September 2025.

[217] Regulation 2021/784 (n 134) Article 2(7).

[218] European Commission, 'Codes of conduct under the Digital Services Act' <https://digital-strategy.ec.europa.eu/en/policies/dsa-codes-conduct> accessed 1 September 2025.

[219] Digital Services Act (n 4) Articles 45-47; this contribution addresses only Article 45.

[220] Rachel Griffin, 'Codes of Conduct in the Digital Services Act: Functions, Benefits & Concerns' (2024) 2024 Technology and Regulation 167, 179.

[221] Digital Services Act (n 4) Article 45(1), see also recital 103: '[…] While the implementation of codes of conduct should be measurable and subject to public oversight, this should not impair the voluntary nature of such codes and the freedom of interested parties to decide whether to participate'.

[222] Griffin, 'Codes of Conduct in the Digital Services Act' (n 220) 175; Jacob van de Kerkhof, 'Jawboning Content Moderation from a European Perspective' in Charlotte van Oirsouw et al (eds), *European Yearbook of Constitutional Law: Constitutional law in the Digital Era, vol 5* (TMC Asser Press 2024).

[223] Digital Services Act (n 4) recitals 103-104. It continues by stating that the mere fact of participation in a code of conduct does not create a presumption of compliance with this Regulation.

checkers.[224] These interactions should generally not lead to exclusion of the liability exemption in light of Article 7 DSA.

However, codes of conduct can also create expectations on the turnaround times of notices, for example explicitly in the Code of Conduct on Countering Illegal Hate Speech+.[225] The question is whether voluntary codes of conduct are capable of affecting the level of diligence required in light of the liability exemption of Article 6(1)(b) – is it possible for hosting providers to become liable after not abiding by a voluntary standard? Based on its monitoring reports, hosting providers have moved to responding to notices within 24 hours, as required by the Code of Conduct, but compliance varies. If expeditiousness by which hosting providers need to address content is interpreted as abiding by industry standards, then not abiding by those industry standards codified in the Code of Conduct may lead to liability for hosting illegal content, as it alters the duty of care for hosting providers on notices for illegal content. It is unclear whether these systemic obligations – 24 hours is a requirement generally, but not for notices specifically – can be extrapolated to individual liability cases. This remains to be seen in practice, but it is not impossible that courts will use codes of conduct to interpret what duty of care is expected from hosting providers, and use the norms set out therein to evaluate content moderation practices of hosting providers.

4.3 SYNTHESIS

Section 2.1 has given an overview of the current practice regarding intermediary liability exemption, and explained the ratio behind the exemption. The scope of intermediary liability exemption is explained broadly in CJEU case law. However, in *L'Oreal* and *YouTube,* the CJEU has been ambiguous in creating a duty of care for hosting providers. The DSA acknowledges that duty of care somewhat, but separates it from liability exemption. Intermediary liability exemption facilitates economic growth and prevents situations in which strict liability of hosting providers would cause harms to freedom of expression. However, Section 3 has illustrated that there are factors that require, and allow, a rethinking of *how* the standard of liability exemption is applied; although the phrasing of the liability exemption has remained relatively unchanged since the ECD, the landscape around that exemption has. Section 4 has explored provisions in the framework of the DSA and sectoral regulation that guide the interpretation of the intermediary liability exemption, and argues that negligent platforms can be excluded from the definition of hosting provider, and that duties of care created in the DSA and sectoral regulation can factually lower the threshold of awareness of illegal content thus triggering Article 6(1)(b).

How does this argument reconcile with concerns for freedom of expression, prohibitions on general monitoring, and the Good Samaritan as outlined in Section 2.2? The suggestions above do not seek to exclude good faith hosting providers from liability exemption; it seeks to exclude bad faith hosting providers. The interpretation of the provisions addressed in this section and their effect on the liability exemption should not be inconsistent with the prohibition on general monitoring obligations. They may lead hosting

[224] European Commission, '2022 Strengthened Code of Practice on Disinformation' (16 June 2022), Commitment 21 <https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation> accessed 1 September 2025.
[225] Code of conduct on Countering Illegal Hate Speech Online + (n 61) 2.3.

providers to monitor for identical or similar content as opposed to the exact illegality when the nature of illegality described in the notice requires such an intervention. They may also require hosting providers to monitor users that frequently upload manifestly illegal content. Neither option contravenes the prohibition on general monitoring obligations of Article 8 as it is interpreted in CJEU case law. The Good Samaritan of Article 7 protects hosting providers from being excluded from liability exemption for acquiring knowledge or awareness in good faith investigations on illegal content. Such may occur for example when investigating users under Article 23, or fulfilling due diligence obligations under Codes of Conduct. However, Article 7 does not protect against liability for not being expeditious in removing such illegal content.[226] It merely ascertains that hosting providers remain neutral after undertaking measures to comply with requirements set by Union law or national law.

The most contingent point in this argumentation is the protection of freedom of expression: many fear that strict(er) liability can chill freedom of expression, as platforms will likely over-remove content to avoid liability.[227] Empirical data on this phenomenon can be divisive in the context of other regulations, for example in the case of *NetzDG*.[228] However, freedom of expression is not an absolute right, and needs to be balanced against other interests.[229] In its case law, the ECtHR has balanced the right to freedom of expression against people's right to private life,[230] but also included considerations whether someone's expressions, if they are considered hate speech, may undermine a cohesive society or suppress minorities.[231] This balancing act may be used to argue for better moderation practices by hosting providers, but it needs to be made carefully to prevent over-removal. The suggestions made above for more diligence by the hosting provider arguably stay within the limit set by the ECtHR for respecting the freedom of expression: the suggestions address gross negligence by the hosting provider, not small issues of non-compliance by *bona fide* hosting providers.

Finally, a note on proportionality. A narrow interpretation of liability exemption in line with additional requirements for diligence may be overly burdensome for smaller hosting providers. Although the requirements of Article 16 DSA also apply to micro-enterprises and smaller enterprises, many of the suggestions made above are also dependent on the position of the hosting provider. In case-by-case analyses, the capacity of smaller enterprises to meet the requirements laid out above can be weighed against the interests of aggrieved parties. This can be done in line with article 19 DSA, for example.

---

[226] Kuczerawy, 'The Good Samaritan That Wasn't' (n 100).
[227] E.g. Kuczerawy, 'The Power of Positive Thinking Special Issues' (n 7); Buiten, De Streel, and Peitz (n 121) 161.
[228] E.g. 'Preventing "Torrents of Hate" or Stifling Free Expression Online?' (The Future of Free Speech 2024) <https://futurefreespeech.org/wp-content/uploads/2024/05/Preventing-Torrents-of-Hate-or-Stifling-Free-Expression-Online-The-Future-of-Free-Speech.pdf> accessed 1 September 2025; Martin Eifert (ed), *Netzwerkdurchsetzungsgesetz in Der Bewährung: Juristische Evaluation Und Optimierungspotenzial* (1. Auflage, Nomos 2020); William Echikson and Olivia Knodt, 'Germany's NetzDG: A Key Test for Combatting Online Hate' (Centre for European Policy Studies 2018, 2018/09) <https://aei.pitt.edu/95110/1/RR_No2018-09_Germany's_NetzDG.pdf> accessed 1 September 2025.
[229] *Handyside v the United Kingdom,* App no 5493/72 (EctHR, 7 December 1976) para 49.
[230] E.g. Case C-131/12 *Google Spain v Mario Gonzalez,* EU:C:2014:317; *Delfi v Estonia* (n 6) para 139; *Biancardi v Italy,* App no 77419/16 (ECtHR, 25 February 2022) para 69.
[231] E.g. *Vejdeland et al v Sweden,* App no 1813/07 (ECtHR, 9 May 2012) paras 56-57.

5 CONCLUSION

The liability exemption for hosting providers in the ECD was adopted almost *verbatim* in Articles 4-6 DSA. Conditional liability exemption provides an adequate but delicate balancing act between the interests of parties affected by illegal content, platform providers requiring legal certainty from being liable for illegal content and the general public, who have an interest in not being subjected to editorial control on the internet potentially constraining their freedom of expression. However, the standards developed around the application of the liability exemption stem from the early 2000s. In the meantime, platforms have developed into sophisticated networks where people can socialise, shop, and take part in the democratic debate, all at the same time. Hosting providers have gained economically from hosting illegal content and have developed sophisticated content moderation mechanisms. The current geopolitical climate puts effective content moderation under pressure. This article argues that, in light of these developments, we must rethink whether our interpretation of the liability exemption regime should evolve within the framework of the DSA.

The DSA introduces a range of due diligence obligations that encourage hosting providers to take more responsibility regarding their content moderation. Several provisions create implicit and explicit duties of care, both in the DSA or by sectoral regulation, and can factor into whether a service qualifies as a hosting provider or whether it has met the threshold of awareness of illegal content. It is important to balance this interpretation on a case-by-case basis. The EU regulator had solid arguments for maintaining the conditional intermediary liability exemption; narrowing the application of the liability exemption requires balancing it with the prohibition on general monitoring *ex* Article 8 DSA and the freedom of expression of internet users. However, in order to ensure a functioning right to freedom of expression, we need a functioning public sphere, which can be achieved through better combatting illegal content online and providing adequate remedies to aggrieved parties. Narrowing the scope of the intermediary liability exemption may be a tool to achieve that, by incentivising platforms to take better care of their due diligence obligations and to better facilitate notice-and-takedown by users. Hosting providers have evolved significantly since the early 2000s; content moderation has evolved synchronously. Perhaps the intermediary liability exemption can evolve too.

LIST OF REFERENCES

Ananny M and Crawford K, 'Seeing without Knowing: Limitations of the Transparency Ideal and Its Application to Algorithmic Accountability' (2018) 20(3) New Media & Society 973
DOI: https://doi.org/10.1177/1461444816676645

Angelopoulos C and Smet S, 'Notice-and-Fair-Balance: How to Reach a Compromise between Fundamental Rights in European Intermediary Liability' (2016) 8(2) Journal of Media Law 266
DOI: https://doi.org/10.1080/17577632.2016.1240957

Berbec A, 'To What Extent Can Online Service Providers Adopt Voluntary Content Moderation Measures without Losing Their Immunity Shields? A Comparative Analysis of Online Service Providers' Liabilities in the European Union and the United States' (2024) 15(1) Journal of Intellectual Property, Information Technology and E-Commerce Law 13

Bertaglia T, Goanta C, and Iamnitchi A, 'The Monetisation of Toxicity: Analysing YouTube Content Creators and Controversy-Driven Engagement' (4th International Workshop on Open Challenges in Online Social Networks, Association for Computing Machinery 2024) <https://dl.acm.org/doi/10.1145/3677117.3685005> accessed 1 September 2025
DOI: https://doi.org/10.1145/3677117.3685005

Bridy A, 'The Price of Closing the "Value Gap": How the Music Industry Hacked EU Copyright Reform' (2020) 22(2) Vanderbilt Journal of Entertainment & Technology Law 323

Broughton Micova S and Kukliš L, 'Responsibilities of Video-Sharing Platforms and Their Users' in Ranaivoson H, Broughton Micova S, and Raats T (eds), *European Audiovisual Policy in Transition* (Routledge 2023)
DOI: https://doi.org/10.4324/9781003262732-8

Brunner L, 'The Liability of an Online Intermediary for Third Party Content: The Watchdog Becomes the Monitor: Intermediary Liability after *Delfi v Estonia*' (2016) 16(1) Human Rights Law Review 163
DOI: https://doi.org/10.1093/hrlr/ngv048

Buiten MC, de Streel A, and Peitz M, 'Rethinking Liability Rules for Online Hosting Platforms' (2020) 28(2) International Journal of Law and Information Technology 139
DOI: https://doi.org/10.1093/ijlit/eaaa012

Casarosa F, 'When the Algorithm Is Not Fully Reliable: The Collaboration between Technology and Humans in the Fight against Hate Speech' in Micklitz HW et al (eds), *Constitutional Challenges in the Algorithmic Society* (Cambridge University Press 2021) DOI: https://doi.org/10.1017/9781108914857.016

Castets-Renardt C, 'Algorithmic Content Moderation on Social Media in EU Law: Illusion of Perfect Enforcement' (2020) 2020(2) University of Illinois Journal of Law Technology & Policy 283

Cauffman C and Goanta C, 'A New Order: The Digital Services Act and Consumer Protection' (2021) 12(4) European Journal of Risk Regulation 758 DOI: https://doi.org/10.1017/err.2021.8

Crawford K and Gillespie T, 'What Is a Flag for? Social Media Reporting Tools and the Vocabulary of Complaint' (2016) 18(3) New Media & Society 410 DOI: https://doi.org/10.1177/1461444814543163

De Gregorio G, 'Expressions on Platforms' (2018) 2(3) European Competition and Regulatory Law Review 203 DOI: https://doi.org/10.21552/core/2018/3/7

De Streel A, 'Online Platforms' Moderation of Illegal Content Online' (European Parliament 2020, PE 652.718) <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652718/IPOL_STU(2020)652718_EN.pdf>accessed 1 September 2025

Dunn P, 'Online Hate Speech and Intermediary Liability in the Age of Algorithmic Content Moderation' (PhD thesis, University of Bologna 2024)

Echikson W and Knodt O, 'Germany's NetzDG: A Key Test for Combatting Online Hate' (Centre for European Policy Studies 2018, 2018/09) <https://aei.pitt.edu/95110/1/RR_No2018-09_Germany's_NetzDG.pdf> accessed 1 September 2025

Edwards L and Veale M, 'Slave to the Algorithm? Why a Right to an Explanation Is Probably Not the Remedy You Are Looking For' (2017) 16(1) Duke Law & Technology Review 18

Eifert M (ed), *Netzwerkdurchsetzungsgesetz in Der Bewährung: Juristische Evaluation Und Optimierungspotenzial* (1. Auflage, Nomos 2020) DOI: https://doi.org/10.5771/9783748909477-207

FitzGerald M, 'Not hollowed by a Delphic frenzy: European intermediary liability from the perspective of a bad man: A response to Martin Husovec et al.' (2025) 32(1) Maastricht Journal of European and Comparative Law 47
DOI: https://doi.org/10.1177/1023263x251316996

Frosio G and Husovec M, 'Accountability and Responsibility of Online Intermediaries' in Frosio G (ed), *The Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020)
DOI: https://doi.org/10.1093/oxfordhb/9780198837138.013.31

Geiger C and Jütte BJ, 'Platform Liability Under Art. 17 of the Copyright in the Digital Single Market Directive, Automated Filtering and Fundamental Rights: An Impossible Match' (2021) 70(6) GRUR International 517
DOI: https://doi.org/10.1093/grurint/ikab037

Geiger C, Frosio G, and Izyumenko E, 'Intermediary Liability and Fundamental Rights' in Giancarlo Frosio (ed), *Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020)
DOI: https://doi.org/10.1093/oxfordhb/9780198837138.013.7

Gellert R and Wolters P, 'The Revision of the European Framework for the Liability and Responsibilities of Hosting Service Providers' (Ministry of Economic Affairs and Climate Policy 2021)

Gillespie T, 'Content Moderation, AI, and the Question of Scale' (2020) 7(2) Big Data & Society 1
DOI: https://doi.org/10.1177/2053951720943234

Goanta C, 'The New Social Media: Contracts, Consumers, and Chaos' (2023) 108 Iowa Law Review 118

Gorwa R, Binns R, and Katzenbach C, 'Algorithmic Content Moderation: Technical and Political Challenges in the Automation of Platform Governance' (2020) 7(1) Big Data & Society 1
DOI: https://doi.org/10.1177/2053951719897945

Griffin R, 'Public and Private Power in Social Media Governance: Multistakeholderism, the Rule of Law and Democratic Accountability' (2023) 14(1) Transnational Legal Theory 46
DOI: https://doi.org/10.1080/20414005.2023.2203538

— —, 'Codes of Conduct in the Digital Services Act: Functions, Benefits & Concerns' (2024) 2024 Technology and Regulation 167
DOI: https://doi.org/10.71265/a54szq76

Heldt A, 'Reading between the Lines and the Numbers: An Analysis of the First NetzDG Reports' (2019) 8(2) Internet Policy Review <https://policyreview.info/articles/analysis/reading-between-lines-and-numbers-analysis-first-netzdg-reports> accessed 1 September 2025
DOI: https://doi.org/10.14763/2019.2.1398

Hickey D et al, 'X under Musk's Leadership: Substantial Hate and No Reduction in Inauthentic Activity' (2025) 20(2) PLOS ONE e0313293
DOI: https://doi.org/10.1371/journal.pone.0313293

Hofmann F and Raue B (eds), *Digital Services Act: Article-by-Article Commentary* (Nomos 2025)
DOI: https://doi.org/10.5771/9783748931478

Holznagel D, 'Chapter II Des Vorschlags Der EU-Kommission Für Einen Digital Services Act — Versteckte Weichenstellungen Und Ausstehende Reparaturen Bei Den Regelungen Zu Privilegierung, Haftung & Herkunftslandprinzip Für Provider Und Online-Plattformen' (2021) 37(2) Computer und Recht 123
DOI: https://doi.org/10.9785/cr-2021-370209

— —, 'Nach dem EuGH-Urteil in Sachen YouTube/Cyando: Fast alles geklärt zur Host-Provider-Haftung?' (2021) 37(9) Computer und Recht 603
DOI: https://doi.org/10.9785/cr-2021-370912

— —, 'How to Apply the Notice and Action Requirements under Art. 16(6) Sentence 1 DSA – Which Action Actually?' (2024) 25(6) Computer Law Review International 172
DOI: https://doi.org/10.9785/cri-2024-250604

Husovec M et al, 'Grand confusion after *Sanchez v. France*: Seven reasons for concern about Strasbourg jurisprudence on intermediaries' (2024) 31(3) Maastricht Journal of European and Comparative Law 385 DOI: https://doi.org/10.1177/1023263x241268436

Husovec M, 'The Promises of Algorithmic Copyright Enforcement: Takedown or Staydown? Which Is Superior? And Why?' (2018) 42(1) Columbia Journal of Law & the Arts 53

— —, 'Mandatory Filtering Does Not Always Violate Freedom of Expression: Important Lessons from *Poland v. Council and European Parliament*' (2023) 60(1) Common Market Law Review 173
DOI: https://doi.org/10.54648/cola2023007

— —, 'Rising Above Liability: The Digital Services Act as a Blueprint for the Second Generation of Global Internet Rules' (2023) 38 Berkeley Technology Law Journal 883

— —, *Principles of the Digital Services Act* (Oxford University Press 2024)
DOI: https://doi.org/10.1093/law-ocl/9780192882455.001.0001

Janal R, 'Haftung Und Verantwortung Im Entwurf Des Digital Services Acts' [2021] Zeitschrift für Europäisches Privatrecht 227

Keller D, 'Dolphins in the Net: Internet Content Filters and the Advocate General's Glawischnig-Piesczek v. Facebook Ireland Opinion' (Stanford Center for Internet and Society, 4 September 2019) <https://cyberlaw.stanford.edu/content/files/2024/05/Dolphins-in-the-Net-AG-Analysis.pdf> accessed 1 September 2025

Kosseff J, *The Twenty-Six Words That Created the Internet* (Cornell University Press 2019)
DOI: https://doi.org/10.7591/9781501735783

Kuczerawy A, 'Intermediary Liability & Freedom of Expression: Recent Developments in the EU Notice & Action Initiative' (2015) 31(1) Computer Law & Security Review 46
DOI: https://doi.org/10.1016/j.clsr.2014.11.004

— —, 'The Power of Positive Thinking Special Issues: Intermediary Liability as a Human Rights Issue' (2017) 8(3) Journal of Intellectual Property, Information Technology and Electronic Commerce Law 226

— —, 'From "Notice and Takedown" to "Notice and Stay Down": Risks and Safeguards for Freedom of Expression' in Frosio G (ed), *Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020)
DOI: https://doi.org/10.1093/oxfordhb/9780198837138.013.27

Lefouili Y and Madio L, 'The Economics of Platform Liability' (2022) 53 European Journal of Law and Economics 319
DOI: https://doi.org/10.1007/s10657-022-09728-7

Madiega T, 'Reform of the EU Liability Regime for Online Intermediaries: Background on the Forthcoming Digital Services Act : In Depth Analysis.' (European Parliament 2019, PE 649.404) <https://data.europa.eu/doi/10.2861/08522> accessed 1 September 2025
DOI: https://doi.org/10.2861/08522

Maroni M, 'The Liability of Internet Intermediaries and the European Court of Human Rights' in Petkova B and Ojanen T (eds), *Fundamental Rights Protection Online* (Edward Elgar Publishing 2020)
DOI: https://doi.org/10.4337/9781788976688.00022

Montagnani ML, 'A New Liability Regime for Illegal Content in the Digital Single Market Strategy' in Frosio G (ed), *The Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020)
DOI: https://doi.org/10.1093/oxfordhb/9780198837138.013.15

Nordemann JB, 'Haftung von Providern im Urheberrecht Der aktuelle Stand nach dem EuGH-Urteil v. 12. 7. 2011 – C-324/09 – L'Oréal/eBay' [2011] GRUR 977

Peguera M, 'The DMCA Safe Harbors and Their European Counterparts: A Comparative Analysis of Some Common Problems' (2008) 32(4) Columbia Journal of Law and the Arts 481

Pollicino O, 'European Judicial Dialogue and the Protection of Fundamental Rights in the New Digital Environment: An Attempt at Emancipation and Reconciliation' in Morano-Foadi S and Vickers L (eds), *Fundamental Rights in the EU: A Matter for Two Courts* (Bloomsbury Publishing 2015)
DOI: https://doi.org/10.5040/9781474202602.ch-006

Quintais JP and Schwemer SF, 'The Interplay between the Digital Services Act and Sector Regulation: How Special Is Copyright?' (2022) 13(2) European Journal of Risk Regulation 191
DOI: https://doi.org/10.1017/err.2022.1

Quintais JP et al, 'Safeguarding User Freedoms in Implementing Article 17 of the Copyright in the Digital Single Market Directive Statements' (2019) 10(3) Journal of Intellectual Property, Information Technology and Electronic Commerce Law 277

Raue B and Heesen H, 'Raue/Heesen: Der Digital Services Act' [2022] Neue Juristische Wochenschrift 3537

Riordan R, 'A Case Study of Judicial-Legislative Interactions via the Lens of the DSA's Host Liability Rules' (2025) 10(1) European Papers – A Journal on Law and Integration 259
DOI: https://doi.org/10.15166/2499-8249/832

Rishabh Kaushal et al, 'Automated Transparency: A Legal and Empirical Analysis of the Digital Services Act Transparency Database' (The 2024 ACM Conference on Fairness, Accountability, and Transparency) <https://dl.acm.org/doi/10.1145/3630106.3658960> accessed 1 September 2025
DOI: https://doi.org/10.1145/3630106.3658960

Sekwenz MT, Wagner B, and Parkin S, "'It Is Unfair, and It Would Be Unwise to Expect the User to Know the Law!" – Evaluating Reporting Mechanisms under the Digital Services Act' (Proceedings of the 2025 ACM Conference on Fairness, Accountability, and

Transparency, Association for Computing Machinery 2025)
<https://dl.acm.org/doi/10.1145/3715275.3732036> accessed 1 September 2025
DOI: https://doi.org/10.1145/3715275.3732036

Senftleben M and Angelopoulos C, 'The Odyssey of the Prohibition on General Monitoring Obligations on the Way to the Digital Services Act: Between Article 15 of the e-Commerce Directive and Article 17 of the Directive on Copyright in the Digital Single Market' (*SSRN*, 4 January 2021)
<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3717022> accessed 1 September 2025

Senftleben M, Quintais JP, and Meiring A, 'How the EU Outsources the Task of Human Rights Protection to Platforms and Users: The Case of UGC Monetization' (2023) 38(3) Berkeley Technology Law Journal 101
DOI: https://doi.org/10.15779/Z381G0HW20

Spindler G, 'The Liability System of Art. 17 DSMD and National Implementation: Contravening Prohibition of General Monitoring Duties' (2019) 10(3) Journal of Intellectual Property, Information Technology and Electronic Commerce Law 344

Trujillo, Fagni T, and Cresci S, 'The DSA Transparency Database: Auditing Self-Reported Moderation Actions by Social Media' (2025) 9(2) Proceedings of the ACM on Human-Computer Interaction 1
DOI: https://doi.org/10.1145/3711085

Ullrich C, 'Standards for Duty of Care: Debating Intermediary Liability from a Sectoral Perspective' (2017) 8(2) Journal of Intellectual Property, Information Technology and Electronic Commerce Law 111

van de Kerkhof J, 'Jawboning Content Moderation from a European Perspective' in van Oirsouw C et al (eds), *European Yearbook of Constitutional Law: Constitutional law in the Digital Era, vol 5* (TMC Asser Press 2024)
DOI: https://doi.org/10.1007/978-94-6265-647-5_4

van de Kerkhof J, 'Musk, Techbrocracy and Free Speech' in Alemanno A and Veraldi J (eds), *Musk, Power, and the EU: Can EU Law Tackle the Challenges of Unchecked Plutocracy?* (Verfassungsbooks 2025)

van Dijck J, *The Culture of Connectivity: A Critical History of Social Media* (Oxford University Press 2013)
DOI: https://doi.org/10.1093/acprof:oso/9780199970773.001.0001

van Drunen MZ, 'The Post-Editorial Control Era: How EU Media Law Matches Platforms' Organisational Control with Cooperative Responsibility' (2020) 12(2) Journal of Media Law 166
DOI: https://doi.org/10.1080/17577632.2020.1796067

van Hoboken J et al, 'Hosting Intermediary Services and Illegal Content Online: An Analysis of the Scope of Article 14 ECD in Light of Developments in the Online Service Landscape' (European Commission 2018) <https://data.europa.eu/doi/10.2759/284542> accessed 1 September 2025
DOI: https://doi.org/10.2759/284542

van Hoboken J, 'The Proposed EU Terrorism Content Regulation: Analysis and Recommendations with Respect to Freedom of Expression Implications' (Transatlantic Working Group on Content Moderation Online and Freedom of Expression 2019) <https://pure.uva.nl/ws/files/46500757/46218669.pdf> accessed 1 September 2025

Vargas Penagos E, 'ChatGPT, Can You Solve the Content Moderation Dilemma?' (2024) 32 International Journal of Law and Information Technology eaae028

Wagner B et al, 'Regulating Transparency?: Facebook, Twitter and the German Network Enforcement Act' (Proceedings of the 2020 ACM Conference on Fairness, Accountability, and Transparency, Association for Computing Machinery 2020) <https://dl.acm.org/doi/10.1145/3351095.3372856> accessed 1 September 2025
DOI: https://doi.org/10.1145/3351095.3372856

Wilman F, 'The EU's System of Knowledge-Based Liability for Hosting Services Providers in Respect of Illegal User Content – Between the e-Commerce Directive and the Digital Services Act' (2021) 12(3) Journal of Intellectual Property, Information Technology and Electronic Commerce Law 317

— —, 'De Digital Services Act (DSA): een belangrijke stap naar betere regulering van onlinedienstverlening' (2022) 28 Nederlands tijdschrift voor Europees Recht 220
DOI: https://doi.org/10.5553/nter/138241202022028009006

— —, 'The Digital Services Act (DSA): An Overview' (*SSRN*, 27 December 2022), 2 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4304586> accessed 1 September 2025
DOI: https://doi.org/10.2139/ssrn.4304586

Wolters P and Gellert R, 'Towards a Better Notice and Action Mechanism in the DSA' (2023) 14(3) Journal of Intellectual Property, Information Technology and Electronic Commerce Law 403

COUNTERING 'LAWFUL BUT AWFUL' DISINFORMATION ONLINE: EU-REGULATIONS TARGETING DISINFORMATION ON MAJOR SOCIAL MEDIA PLATFORMS

THERESE ENARSSON*

This article examines the European Union's regulatory framework for addressing disinformation, with particular focus on the Digital Services Act (DSA) and the responsibilities of Very Large Online Platforms (VLOPs) and so-called 'lawful but awful' disinformation – harmful yet legal content. The study highlights how the EU avoids content censorship by emphasising systemic risk assessment and mitigation. Notably, disinformation is rarely defined with precision yet is framed as especially problematic when linked to democratic processes, political advertising or crises.

A key finding is the Commission's reliance on soft law to steer platform behaviour. By pushing for soft law instruments the EU can expand some normative influence without crossing into formal content regulation. While VLOPs face substantial responsibilities, the enforcement of these measures remains uncertain. These frameworks reflect a shift toward platform governance through risk-based regulation and soft law, with the Commission increasingly shaping the moderation of harmful online content without legislating censorship.

1 INTRODUCTION

1.1 BACKGROUND

Disinformation has been identified as the most pressing global risk in the short to medium term by the World Economic Forum, also amplifying other risks like state-based armed conflict and extreme weather.[1] In Europe, the European Commission has also identified disinformation as a threat to society and has responded through different means, by using a 'whole-of-society approach',[2] stating that many actors and sectors play a role in countering disinformation. The focus in this article is to analyse one main and fundamental approach by the EU to targeting disinformation – the use of regulatory measures to increase the responsibilities of Very Large Online Platforms (VLOPs).[3]

---

* Associate Professor, Department of Law, Umeå University. ORCID-id: 0000-0003-1184-1385; LinkedIn: https://se.linkedin.com/in/therese-enarsson-bb8a6251; therese.enarsson@umu.se. This work was supported by the Swedish Research Council [grant numbers 2020-02278 and 2022-05414]. No potential conflict of interest was reported by the author.

[1] Mark Elsner, Grace Atkinson, and Saadia Zahidi, 'Global Risks Report 2025' (*World Economic Forum*, 15 January 2025), 4, 8 and 13 <https://www.weforum.org/publications/global-risks-report-2025/digest/> accessed 1 September 2025.

[2] European Commission, 'Strategic Communication and Countering Information Manipulation' (2025) <https://commission.europa.eu/topics/countering-information-manipulation_en> accessed 1 September 2025.

[3] Very Large Online Platforms are here defined in accordance with art 33(1) of the DSA, as online platforms with more than 45 million users. (The same amount of average monthly users defines a Very Large Online Search Engine 'VLOSE').

The dissemination of false and deceptive information to influence public opinion, incite violence or achieve commercial gain is not a new phenomenon. Nor is the widespread circulation of disinformation via social media platforms. What has changed, however, is the arena in which disinformation spreads and the ways it shapes its impact. The digital sphere not only accelerates the dissemination of disinformation but also enables it to reach wide audiences and target specific groups with precision. This has made disinformation a more pervasive and intense societal phenomenon.[4]

One notable example of the challenge posed by disinformation is the phenomenon of filter bubbles – situations where algorithms tailor users' experiences to their existing preferences, thereby reinforcing pre-existing beliefs and perspectives.[5] As a result, people may become increasingly misinformed, caught in a bubble of disinformation – often a mixture of half-truth, falsehoods, and value judgments – reinforced by algorithms and echoed within communities of like-minded individuals.[6] This environment can even draw users into a 'rabbit hole' of disinformation, pushing them toward deeper misinformed, or even radicalized, states.[7]

Disinformation often spreads through processes of algorithmic recommendation and amplification, gradually fostering discord, polarization and radicalization. It does so by employing manipulative tactics designed to maximize user engagement and platform usage.[8] It has also been shown that disinformation plays on strong – and often negative – emotions, which in turn increase both the reach of such content and the intensity of users' interaction with it.[9] Beyond emotional manipulation, the digital sphere enables new forms of behaviour and communication that traditional media cannot, with algorithms amplifying content and non-human actors, such as bots, disseminating material at scale, often simulating human interaction. This combination significantly increases the risks to democratic processes, electoral integrity, and civic discourse.[10]

In response to the societal challenges posed by disinformation, the Digital Services Act (DSA) stands out as the most significant legislative measure, establishing the world's first binding regulatory framework that compels the largest digital platforms to take responsibility for the spread and impact of harmful content online. This makes the EU the first jurisdiction in the world to set such standards. The DSA specifically places stricter responsibilities on

---

[4] Emiliana De Blasio and Donatella Selva, 'Who Is Responsible for Disinformation? European Approaches to Social Platforms' Accountability in the Post-Truth Era' (2021) 65 American Behavioral Scientist 825, 828.
[5] Eli Pariser, *The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think* (Penguin Books Ltd 2011).
[6] Carlos Diaz Ruiz and Tomas Nilsson, 'Disinformation and Echo Chambers: How Disinformation Circulates on Social Media Through Identity-Driven Controversies' (2023) 42(1) Journal of Public Policy & Marketing 18.
[7] Becca Lewis, 'Rabbit Hole: Creating the Concept of Algorithmic Radicalization' in Johan Farkas and Marcus Maloney (eds) *Digital Media Metaphors* (Routledge 2024).
[8] Will Mbioh, 'Beyond Echo Chambers and Rabbit Holes: Algorithmic Drifts and the Limits of the Online Safety Act, Digital Services Act, and AI Act' (2024) 33(3) Griffith Law Review 189.
[9] Steffen Steinert and Matthew James Dennis, 'Emotions and Digital Well-Being: On Social Media's Emotional Affordances' (2022) 35 Philosophy & Technology 36; Mbioh (n 9).
[10] Philip N Howard and Bence Kollanyi, 'Bots, #Strongerin, and #Brexit: Computational Propaganda During the UK-EU Referendum' (*SSRN*, 20 June 2016), 5 <https://papers.ssrn.com/abstract=2798311> accessed 1 September 2025; Andrew Peck, 'A Problem of Amplification: Folklore and Fake News in the Age of Social Media' (2020) 133(529) Journal of American Folklore 329.

VLOPs.[11] In the DSA, it is pointed out that these dominant platforms '[…] can be used in a way that strongly influences safety online, the shaping of public opinion and discourse'.[12] This is a relevant backdrop to understanding how the regulation is supposed to impact illegal or harmful content online, such as disinformation.

As part of the same emerging regulatory field as the DSA, the Council of the European Union approved the EU Artificial Intelligence Act (the 'AI Act') in May 2024.[13] This is the first comprehensive legal framework in the world regulating AI. This regulation will also have some impact on how VLOPs are expected to work with content that can be considered disinformation, most importantly generative AI such as *deepfakes* – manipulated content depicting real people or events that does not necessarily appear to be manipulated to a regular social media user online.[14]

Besides these overarching frameworks, there are several instruments, both hard and soft law, which the Commission itself identifies as targeting disinformation by increasing responsibilities for VLOPs.[15] They especially target areas of hate speech,[16] terrorist propaganda[17] and political advertisement.[18] The latter area has only in recent years received attention as part of overarching EU regulation targeting the online sphere due to the security implications of misleading advertisement.[19]

For the purposes of this article, there is a particularly important soft law instrument addressing disinformation – the Code of Practice on Disinformation – which, as of July 1st, 2025, became a formal code of conduct under the DSA.[20] This instrument is described as becoming '[…] a relevant benchmark for determining DSA compliance regarding disinformation risks for the providers of VLOPs and Very Large Online Search Engines (VLOSEs) that adhere to and comply with its commitments' by the European Commission,

---

[11] There are specific responsibilities placed on very large online search engines in the DSA as well, but search engines will not be included in this study.
[12] 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) [2022] OJ L277/1 recital 79.
[13] Regulation (EU) 2024/1689 of the European Parliament and of the Council 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) [2024] OJ L2024/1689.
[14] ibid recital 134.
[15] European Commission, 'Strengthening Online Platforms' Responsibility' <https://commission.europa.eu/topics/countering-information-manipulation/strengthening-online-platforms-responsibility_en> accessed 1 September 2025.
[16] European Commission, 'The EU Code of Conduct on Countering Illegal Hate Speech Online' <https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en> accessed 1 September 2025.
[17] Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online [2021] OJ L172/79.
[18] Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising [2024] OJ L2024/900 (Regulation on the transparency and targeting of political advertising).
[19] Benjamin Farrand, 'Regulating Misleading Political Advertising on Online Platforms: An Example of Regulatory Mercantilism in Digital Policy' (2024) 45(5) Policy Studies 730, 730–731.
[20] European Commission, 'The Strengthened Code of Practice on Disinformation 2022' (16 June 2022), 1(h) <https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation> accessed 1 September 2025; European Commission, 'The Code of Conduct on Disinformation' (13 February 2025) <https://digital-strategy.ec.europa.eu/en/library/code-conduct-disinformation> accessed 1 September 2025.

and it is expected to play a significant role in understanding the demands under the DSA.

This wide regulatory approach targeting disinformation is an indicator of an equally wide concept – consisting of acts with vastly different gravity and intent. Disinformation can often be placed in the category of online content that is 'lawful but awful', since disinformation is not necessarily illegal, and it can be understood as the act of intentionally spreading misleading information, potentially causing harm.[21] It is important to note, however, that disinformation may also constitute illegal content, such as hate speech or terrorist propaganda.[22]

Yet, disinformation can be perceived as something much wider than just the spread of illegal material, relating to anything from health and religion to beauty products. It that sense, *disinformation* as a term can be said to have an umbrella character, and disinformative content can spread in different ways with different intent and impact.[23] Legally, more specific definitions of disinformation and its possible illegality must therefore be determined at the national level of EU Member State, some of which already have regulation in place to counter or ban certain defined forms of disinformation,[24] and in some cases through EU-level legislation.

The issue of illegality is closely linked to the liability of VLOPs for the content they host. Under the EU's approach, VLOPs are not held liable for failing to moderate content unless they have been notified of its illegality.[25] This also means that platforms are not explicitly obligated to monitor their services,[26] even if case law from the ECtHR and the ECJ indicates that a level of monitoring is necessary, though only for some illegal content.[27]

The Commission has also emphatically stated that it has no intention of censoring content or deciding what the truth is online. Focusing on platform regulation and platforms' responsibilities to maintain a safe space for users, instead of targeting specific content, has clearly been a way for the EU to balance different interests and rights.[28] Perhaps as a natural

---

[21] For more on this concept of lawful but awful content, see Anastasia Kozyreva et al, 'Resolving Content Moderation Dilemmas between Free Speech and Harmful Misinformation' (2023) 120(7) Proceedings of the National Academy of Sciences e2210666120.

[22] The matter of defining illegality in hate speech is however not straight forward either, but will not be further discussed in this article. It is analyzed in-depth in Therese Enarsson, 'Navigating Hate Speech and Content Moderation under the DSA: Insights from ECtHR Case Law' (2024) 33(3) Information & Communications Technology Law 384.

[23] Tarlach McGonagle and Katie Pentney, 'From Risk to Reward? The DSA's Risk-Based Approach to Disinformation' in Maja Capello et al (eds), *Unravelling the Digital Services Act package* (European Audiovisual Observatory 2021) 44.

[24] Like Germany with The Network Enforcement Act 'NetzDG - Gesetz Zur Verbesserung Der Rechtsdurchsetzung in Sozialen Netzwerken' <https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html> accessed 1 September 2025, and France with its' legislation: LOI n°2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information (1) 2018 (2018-1202) stating that judges can authorizes removing political disinformation in relation to election campaigns.

[25] Digital Services Act (n 12) Article 6, see also Article 74(1).

[26] Marcin Rojszczak, 'The Digital Services Act and the Problem of Preventive Blocking of (Clearly) Illegal Content' (2023) 3(2) Institutiones Administrationis – Journal of Administrative Sciences 44, 46-47.

[27] See Enarsson (n 22); *Delfi AS v Estonia* App no 64569/09 (ECtHR, 16 June 2015) para 47; Case C-18/18 *Eva Glawischnig-Piesczek v Facebook Ireland Limited* EU:C:2019:821 paras 39, 41, 45 and 46; Clara Rauchegger and Aleksandra Kuczerawy, 'Injunctions to Remove Illegal Online Content under the Ecommerce Directive: Glawischnig-Piesczek' (*SSRN*, 31 August 2020) <https://papers.ssrn.com/abstract=3728597> accessed 1 September 2025.

[28] Giovanni De Gregorio and Oreste Pollicino, 'The European Approach to Disinformation: Policy Perspectives' (Institute for European Policymaking, June 2024), 2

response to the vague nature of disinformation as a phenomenon and the regulatory instruments targeting it, the DSA – the most comprehensive framework targeting the responsibilities of VLOPs – was criticized even before coming into full effect for not providing clear demands or tools for addressing disinformation, especially such content that might pose a grave risk to society and be harmful, even when not clearly illegal.[29]

It is clear that disinformation is a key concern for the EU in safeguarding democracy and free elections, but it remains unclear how VLOPs should define disinformation and whether, or to what extent, they are obligated to address it. This article contributes to a deeper understanding of how the EU addresses disinformation through regulatory measures – and whether these efforts extend beyond clearly unlawful content. This can add to research on regulatory responses to disinformation, illuminating the role VLOPs are intended to play in targeting such harmful but lawful content.

1.2 AIM, METHOD AND CONTRIBUTION

This article will therefore focus on three, intertwining, questions:

1) *How is disinformation specified or framed in new regulatory instruments?*
   This research question focuses on the content, actions or types of disinformation that are targeted in these instruments but *not* classified as illegal per se (i.e. hate speech and terrorism propaganda).
2) *What regulatory demands are directed at VLOPs to target or counter disinformation on their platform?*
   This research question specifically targets correlating demands for actions taken by VLOPs as a response to disinformation, as identified above. What content, actions or types of disinformation is to be targeted and how?
3) *What does this indicate regarding the role of VLOPs in countering the dissemination of disinformation in the online sphere, and in turn, what does that say about the regulatory approach used by the EU to target 'lawful but awful' content?*
   This final analysis aims to shed light on whether specific disinformative actions, content or contexts can be identified in these instruments, spanning beyond clearly unlawful content and aiming to clarify the perceived and intended role of VLOPs in the whole-of-society approach to disinformation.

To address these questions, a textual and qualitative analysis of legal material will be conducted, combining a doctrinal analysis with a normative evaluation, focusing on the DSA and, to a lesser extent, the AI Act and the Regulation on the transparency and targeting of political advertising.[30] The AI Act has a limited interplay with regulating disinformation on social media platforms but will be analysed in relation to generative AI, especially regarding risk assessment and risk mitigation in relation to, and as regulated by, the DSA. The Regulation on the Transparency and Targeting of Political Advertising will also be considered

<https://iep.unibocconi.eu/sites/default/files/media/attach/PB19_Disinformation_%20Pollicino.pdf> accessed 1 September 2025.

[29] Ethan Shattock, 'Fake News in Strasbourg: Electoral Disinformation and Freedom of Expression in the European Court of Human Rights (ECtHR)' (2022) 13(1) European Journal of Law and Technology 1.

[30] Regulation on the transparency and targeting of political advertising (n 18).

as part of mapping the emerging regulatory framework on disinformation and will be analysed in relation to the context of disinformative and misleading political ads. The obligation for VLOPs to curtail such content through content moderation is regulated in the DSA, however.[31]

Using that as a point of departure, it will also be necessary to branch out to soft-law instruments, since the area of online regulation is highly directed towards self- and co-regulatory instruments, mainly codes of conduct.[32] Here the Code of Practice on Disinformation will be of particular importance.[33] Taken together, this article aims to establish what legal rules, requirements, or limits are placed on VLOPs to counter disinformation, and how far that reaches beyond clearly illegal content.

Because the DSA and the AI Act are both new regulations in an emerging field, the interpretation and outcome of their implementation could also impact how legislation in other jurisdictions around the world sets out to regulate this worldwide phenomenon.[34]

2 REGULATORY FRAMING OF DISINFORMATION

2.1 DISINFORMATION AS SOCIETAL RISK FOR DEMOCRATIC AND ELECTORAL PROCESSES

As mentioned, the Commission has clearly stated that it will never decide what the truth is online.[35] This has been elaborated on by Martin Husovec, who suggested that demanding VLOPs to target specific, in itself *lawful* content, would be crossing a red line:

> Whenever the Commission tackles problems that are posed also by *lawful* expressions, the mitigation measures that it requires from companies must remain strictly content-neutral. Any attempt by the Commission to prescribe content-specific measures for legal content, such as forcing companies to ban some specific lawful content in terms and conditions, would mean that the Commission assumes the role of a surrogate legislature regarding content. The DSA offers no empowerment for such formal rulemaking. Doing so would mean that the Commission oversteps its competencies. It crosses a red line.[36]

Without being able to define what specific expressions could be disinformative, apart from already unlawful content under national or European legislation, these new regulatory

---

[31] Liubomir Nikiforov, 'Transparency in Targeting of Political Advertising: Challenges Remain' (*SSRN*, 1 November 2024) <https://papers.ssrn.com/abstract=5054430> accessed 1 September 2025.
[32] Rachel Griffin, 'Codes of Conduct in the Digital Services Act: Functions, Benefits & Concerns' (2024) 2024 Technology and Regulation 167.
[33] European Commission, 'The Strengthened Code of Practice on Disinformation 2022' (n 20).
[34] Martin Husovec, 'Rising Above Liability: The Digital Services Act as a Blueprint for the Second Generation of Global Internet Rules' (2023) 38(3) Berkeley Technology Law Journal 884; Anupam Chander, 'When the Digital Services Act Goes Global' (2023) 38(4) Berkeley Technology Law Review 1067; Daphne Keller, 'The EU's New Digital Services Act and the Rest of the World' (*Verfassungsblog*, 7 November 2022) <https://verfassungsblog.de/dsa-rest-of-world/> accessed 1 September 2025; Mateusz Łabuz, 'Regulating Deep Fakes in the Artificial Intelligence Act' (2023) 2(1) Applied Cybersecurity & Internet Governance 1.
[35] Gregorio and Pollicino (n 28).
[36] Martin Husovec, 'The Digital Services Act's Red Line: What the Commission Can and Cannot Do about Disinformation' (2024) 16(1) Journal of Media Law 47, 55.

frameworks still clearly target the spread of disinformation. Therefore, to clarify this broader targeting of disinformation and the demands placed on VLOPs to counter it, it is vital, as a first step, to recognize how disinformation is framed or understood in instruments targeting the phenomenon.

The AI Act and, even more extensively, the DSA frame disinformation as a separate phenomenon from illegal content, and disinformation is understood and described as relating to certain contexts and actions that result in the spread of harmful content. The aim of the DSA – to create safe and trustworthy spaces online – expands the scope beyond simple illegal acts or content.[37] It is clear from the first recitals in the DSA, which frame the aim and purpose of the regulation, that disinformation is viewed and phrased as a risk for society. In recital 2 the efforts or concerns of member States to '*tackle illegal content, online disinformation or other societal risks'* are mentioned, and addressing disinformation as a *societal risk* that can cause *societal harm* is a theme that continues throughout the DSA.[38] This is framed in slightly different ways throughout the DSA, providing guidance on how disinformation is to be understood.

One specific context or type of action that can pose a risk is highlighted in recital 69 DSA, where particular weight is given to users' vulnerabilities being exploited or manipulated through advertising techniques, stating that '[i]n certain cases, manipulative techniques can negatively impact entire groups and amplify societal harms, for example by contributing to disinformation campaigns or by discriminating against certain groups'. Here online platforms are also identified as constituting a higher societal risk than other environments due to the potential for being used for that kind of manipulation.[39] Online platforms are therefore to use neither micro-targeting nor base advertising on the profiling of users, in line with the General Data Protection Regulation (GDPR).[40]

The impact and potential harm of advertising is also reiterated in the Regulation on the Transparency and Targeting of Political Advertising that came into force in 2024.[41] Here, a clear focus is – of course – transparency, more precisely regarding who is advertising, who is paying for ads and for which election. This ties together with safeguarding free elections. An overall objective in the EU is that elections should be free from disinformation and misleading political ads, and the Regulation on the Transparency and Targeting of Political Advertising mirrors that overall aim.[42]

---

[37] Digital Services Act (n 12) recitals 9, 69, 84, 104. See also Artificial Intelligence Act (n 13) recital 110.
[38] Digital Services Act (n 12) recitals 2, 9, 69, 83, 88, 95, 104.
[39] ibid recital 69.
[40] 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, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1 Article 4(4).
[41] Regulation on the transparency and targeting of political advertising (n 18) recital 6.
[42] Directorate-General for Communications Networks, Content and Technology (European Commission), 'A Multi-Dimensional Approach to Disinformation: Report of the Independent High Level Group on Fake News and Online Disinformation' (Publications Office of the European Union 2018) <https://data.europa.eu/doi/10.2759/739290> accessed 1 September 2025; European Commission, 'Strengthening Online Platforms' Responsibility' <https://commission.europa.eu/topics/countering-information-manipulation/strengthening-online-platforms-responsibility_en> accessed 1 September 2025. There is also a new code of conduct underway, specifically targeting political advertisement, potentially adding to the field of countering disinformation, as well as protecting free elections, see Julian Jaursch, 'Addressing Online Advertising Transparency in the DSA and Beyond' (*Tech Policy Press*, 16 December 2024)

In the Regulation on the transparency and targeting of political advertising, disinformation and misleading advertisements are not defined – but through understanding the purpose of the regulation, conclusions can still be drawn on the type of content that is targeted. Here the focus is to prevent deceiving the public while enhancing open political campaigns and debates, and by doing so also protecting a well-functioning democratic society.[43] This is to be done by limiting election interference and opaque political advertising. It is worth noting, however, that the regulation has already received criticism for referring obligations on content moderation to the DSA and for not providing sufficient guidance for moderation systems – automatic or human-based systems – to successfully identify political ads and make nuanced moderation decisions. Moderation of political content will be especially challenging during the most sensitive periods around elections, with massive amounts of content to moderate, which enhances the need for clear guidelines for VLOPs.[44]

The focus on democratic processes and elections is also prominent in the AI Act. While the AI Act takes a back seat to the DSA in relation to more general obligations to fight disinformation, it specifically highlights the prevalence of disinformation in the context of democracy and free elections.[45] The interplay between the DSA and the AI Act is visible in the phrasing of the act, where the importance of effective implementation of the DSA in relation to detection of the use of AI systems is reiterated, stating that VLOPs must identify and mitigate risks connected to AI-manipulated or AI-generated content*,* '[…], in particular risk of the actual or foreseeable negative effects on democratic processes, civic discourse and electoral processes, including through disinformation'.[46]

More specifically, disinformation in the AI Act mainly relates to the prevalence of bots and deepfakes on online platforms. This is defined in Article 3(60) and targets AI-generated or manipulated content that can be interpreted as genuine by those who engage with it. The definition in Article 3 (60) encompasses all types of content – from image, audio or video – that depict or resemble existing persons, material objects or events. It is important to note that, to constitute a deepfake, it must resemble or depict something or someone existing in real life, but with a purpose, or at least potential, to mislead.

Fighting disinformation is thus given a prominent – but vague – place in the DSA and the Regulation on the Transparency and Targeting of Political Advertising and AI Act alike, with no clear definitions of the concept. Instead, these regulations focus on the risks that disinformation can cause to society, democracy and electoral processes as well as the responsibility of VLOPs to be aware of and mitigate those risks.

2.2 DISINFORMATION AS *CONTEXT* AND *ACTIONS*, NOT CONTENT

As a stepping stone toward understanding the obligations to counter disinformation beyond

<https://techpolicy.press/addressing-online-advertising-transparency-in-the-dsa-and-beyond> accessed 1 September 2025.

[43] Regulation on the transparency and targeting of political advertising (n 18) see, inter alia, recitals 7 and 74.

[44] Nikiforov (n 31. For more on the need for contextual moderation decisions, see Therese Enarsson, Lena Enqvist, and Markus Naarttijärvi, 'Approaching the Human in the Loop – Legal Perspectives on Hybrid Human/Algorithmic Decision-Making in Three Contexts' (2022) 31(1) Information & Communications Technology Law 123; Enarsson (n 22).

[45] Artificial Intelligence Act (n 13) recitals 110, 120 and 136.

[46] ibid, recital 120.

clearly illegal content, disinformation should be framed as conduct – such as disinformation campaigns – involving rapid dissemination of content. More precisely, it refers to content situated within or concerning certain contexts, particularly elections and democratic or political processes, which may in various ways pose risks to society or result in societal harm. With that being said, the AI Act and the Regulation on the Transparency and Targeting of Political Advertising are two examples of actions or contexts that have been singled out and provide more narrow and more precise aims for what kind of disinformation is to be targeted – with corresponding mentions in the DSA.

On top of this, the DSA also takes a rather wide approach to disinformation and encourages certain actions, such as awareness-raising efforts in relation to the risks of disinformation campaigns. Another such vital aspect highlighted in the DSA is joining self- and co-regulatory instruments, mainly codes of conduct, to strengthen cooperation in countering harmful content that is spread across several platforms online.[47]

This brings us to the most relevant framework within the EU on countering disinformation on VLOPs, alongside the DSA – the strengthened Code of Practice on Disinformation. The Code of Practice was first signed in 2018 but has since been strengthened in 2022. When developed and strengthened, the Code was updated in accordance with suggestions by the Commission, and the preamble already included an intention to become a code of conduct in the, then future, DSA. As mentioned, the Code became a formal code under the DSA in 2025. Yet, The Code of Practice is not originally a product of the European Commission but was shaped by the Signatories. Initially, it was therefore best understood as a self-regulatory instrument, where private companies voluntarily developed their content, rules and more detailed demands for their practices.[48] However, its current and future status is best understood as a co-regulatory instrument between the Commission and the Signatories of the code.[49]

The use of self- and co-regulatory instruments is part of the network of regulatory instruments targeting the online sphere, and other highly important codes of conduct have emerged, such as the EU Code of Conduct on Countering Illegal Hate Speech Online.[50] One major difference is that the Code of Practice on Disinformation also targets mainly *lawful* speech. This brings us back to defining or understanding what disinformation *is* under the emerging regulatory framework. In the Code of Practice on Disinformation, the scope is very broad, but there are clear definitions of what kinds of *actions* are included, and, to some extent, which *actors*.

Here, the Signatories to the Code, including VLOPs like Meta and TikTok, are required to fight against disinformation, including misinformation, meaning that spreading misleading information in a harmful way, with (or even without) intent to cause harm and to a relatively small circle, is included in this definition, as well as the more obvious understanding of disinformation as a tool to mislead and deceive, often with a specific goal in mind, such as

[47] Digital Services Act (n 12) recital 88.
[48] Tony Porter and Karsten Ronit, 'Self-Regulation as Policy Process: The Multiple and Criss-Crossing Stages of Private Rule-Making' (2006) 39 Policy Sciences 41; Carl Vander Maelen, 'Hardly Law or Hard Law? Investigating the Dimensions of Functionality and Legalisation of Codes of Conduct in Recent EU Legislation and the Normative Repercussions Thereof' (2022) 47(6) European Law Review 752.
[49] European Commission, 'The Strengthened Code of Practice on Disinformation 2022' (n 20); Griffin (n 32) 174.
[50] European Commission, 'The EU Code of Conduct on Countering Illegal Hate Speech Online' (n 16).

political gain. Furthermore, both foreign and domestic campaigns to influence a certain audience for a specific purpose are included in the Code of Practice, as well as efforts to influence or disrupt the free political will of individuals by foreign state actors.[51] This followed after the Commission encouraged such an inclusion.[52]

The broad definitions of disinformation in EU regulatory instruments can be, and have been, criticized for not providing legal certainty and effectiveness, and this vagueness could be problematic when it comes to protecting freedom of expression.[53] At the same time, the European Commission does not wish to censor content, and trying to clarify every action or type of content that could constitute disinformation is of course highly complex, if not impossible. However, how disinformation is presented in these regulatory instruments still provides insight into their purpose.

The focus must be understood as acts of manipulation and the potential risks posed by certain types of content – particularly in contexts such as public health (as will be shown below) and democratic security – rather than on the precise content of the information itself. Perhaps this shows a potential misconception: maybe VLOPs are not meant to identify and analyse disinformation per se, but rather to assess and mitigate risks.

3 RESPONDING TO DISINFORMATION ON VERY LARGE ONLINE PLATFORMS

3.1 DEMANDS TO ASSESS AND MITIGATE *RISKS* OF LAWFUL DISINFORMATIVE ACTIONS

The turn to risk as a parameter is a common trait in regulations affecting the digital domain in recent years, from the GDPR to the DSA and the AI Act. The matters of risk and societal harm are prominent in the DSA and the AI Act alike. Risk assessments and risk mitigation are at the core of the DSA, and the understanding of these concepts is largely connected to risks for society or individuals. Building on the understanding above, where targeting disinformation goes beyond targeting clearly illegal content, the question becomes 'how do obligations to conduct risk assessment and risk mitigation under the DSA apply to lawful contexts and actions of disinformation as presented above?'

Article 34 DSA, regulating risk assessment, and Article 35, regulating risk mitigation, are very broad. The scope of Article 34 and the risk assessments to be made, include the spread of illegal content on the platforms, actual or potential future infringements of fundamental rights, negative effects on civic discourse and electoral processes, as well as public security. Beyond this, VLOPs are to consider actual or foreseeable negative effects regarding gender-based violence, as well as the protection of public health. VLOPs must also

---

[51] European Commission, 'The Strengthened Code of Practice on Disinformation 2022' (n 20) 1 (a) with footnotes.

[52] Sharon Galantino, 'How Will the EU Digital Services Act Affect the Regulation of Disinformation?' (2023) 20(1) SCRIPTed 89, 126; European Commission, 'Guidance on Strengthening the Code of Practice on Disinformation' (last updated 26 January 2023) <https://digital-strategy.ec.europa.eu/en/library/guidance-strengthening-code-practice-disinformation> accessed 1 September 2025.

[53] Ronan Ó Fathaigh, Natali Helberger, and Naomi Appelman, 'The Perils of Legally Defining Disinformation' (2021) 10(4) Internet Policy Review, 18-19 <https://policyreview.info/articles/analysis/perils-legally-defining-disinformation> accessed 1 September 2025.

consider serious negative consequences for a person's physical and mental well-being and protect minors. To describe this as very broad might even be understated. Nonetheless, this broad responsibility shows that VLOPs must conduct risk assessment and mitigation in a wide range of situations that can pose a risk or cause harm to individuals and society, and are therefore risk-based in relation to specific contexts and not explicitly focused on specific content or expressions.[54]

However, to further understand how risk assessment and mitigation in the DSA can apply to disinformation, it is necessary to determine whether disinformation is included in the four categories presented in the DSA that are to be under specific assessment by VLOPs. The categories are: (a) the dissemination of illegal content; (b) any actual or predictable impact of the service on the exercise of fundamental rights; (c) any foreseeable or actual negative effects on democratic processes, civic discourse and electoral processes, or public security; and lastly (d) any actual or foreseeable negative effects relating to the protection of minors, public health or gender-based violence.[55] In different ways, these can all apply to disinformation. As mentioned, disinformation is not automatically defined as illegal but can consist of illegal content or be part of illegal activities, such as spreading terrorist propaganda or illegal hate speech.[56] What is illegal offline should, according to Article 3(h) and recital 12 DSA, be illegal online. As also mentioned, even though disinformation can be classified as illegal content, that is left out of the scope of this article.

Disinformation can also affect the exercise of fundamental rights, for example through aspects mentioned under (c) that can impact free elections. As has been shown so far, this is a clear and expressed aim and focus in the Regulation on the Transparency and Targeting of Political Advertising and the AI Act as well, highlighting that the importance of protecting free elections is part of the reason for countering disinformation.[57] It is also prominently targeted in the Code of Practice on Disinformation. However, it is not expressly referenced in relation to disinformation within the DSA. The European Commission did, however, clarify the need for risk assessment and mitigation leading up to the European Parliament elections in June 2024, though, and highlighted that VLOPs should cooperate with a number of actors, including the EU and national authorities, civil society organizations and other experts to counter disinformation and other manipulation or interference with the election.[58] That VLOPs must guard electoral freedom and identify, analyse and assess interferences with elections is therefore still evident.

The only one of these four categories requiring risk assessment in the DSA that *is* mentioned explicitly in relation to disinformation is the fourth, relating to Article 34(1)(d). In recital 83 it is stated that platforms should assess concerns of manipulation of the

---

[54] Husovec, 'The Digital Services Act's Red Line' (n 36) 47. This is supposed to make the DSA stand the test of time by being content- and technology-neutral.

[55] Digital Services Act (n 12) Articles 34(1)(a)–(d), recitals 80–83. With regard to embedded AI systems or AI models in designated VLOPS, it is worth noting that since VLOPs must follow the risk-management framework provided in the DSA, the same obligations under the AI Act are to be presumed to be fulfilled if taken such measures, if not significant systemic risks stemming from the use of AI is not covered in the DSA are identified (Artificial Intelligence Act (n 13) recital 188).

[56] Enarsson (n 22).

[57] Regulation on the transparency and targeting of political advertising (n 18), see, e.g., recital 4; Artificial Intelligence Act (n 13) recital 120 for example.

[58] European Commission, 'Commission publishes guidelines under the DSA' (press release, 26 March 2024) <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1707> accessed 1 September 2025.

platform, including 'coordinated disinformation campaigns related to public health'. In the following recital 84, it is further stated that VLOPs should not only focus on illegal content, but also on that which is not illegal but contributes to systemic risks, proclaiming that '[…] [p]roviders should therefore pay particular attention on how their services are used to disseminate or amplify misleading or deceptive content, including disinformation'. Recital 83, as well as recital 84, clarify that of risks stemming from the use or design of the service, also relate to inauthentic use of the platforms' services. Here, fake accounts and bots are mentioned as risk factors and ways to rapidly spread either illegal content, or such content that contributes to disinformation campaigns. Acting on conceivable risks is at the core of the AI Act as well, focusing on risks stemming from the use of AI. Here, the AI Act and the DSA are again intertwined.[59]

In recital 136 of the AI Act, it is clarified that the obligations stated in the regulation are crucial for an effective implementation of the DSA, specifying the obligations to enact risk assessment and mitigation of, for instance, disinformation. However, in the AI Act, most of the responsibilities for AI generated content are placed on the deployers[60] or providers[61] of AI systems or models. The AI Act also identifies and classifies AI according to the level of risk a certain system poses to individuals or society, from unacceptable and high risk to limited risk or minimal risk. On this four-step scale, deepfakes generated by AI are classified as a *limited* risk. This means that deployers of, for instance, a deep fake, only have to clarify that the content has been manipulated, 'in an appropriate manner that does not hamper the display or enjoyment of the work'.[62] However, concerns have been raised about this classification for deepfakes due to the transnational nature and potential harms of deepfakes, advocating for a higher level of risk classification.[63] Of course, deepfakes could also be part of widely spread disinformation campaigns that pose a risk to society and individuals, thereby requiring VLOPs to act under the DSA.[64]

Ongoing risk analysis, with corresponding responses from VLOPs, is therefore demanded, even regarding 'lawful but awful' disinformation. It is not the content, its illegality

[59] See Artificial Intelligence Act (n 13) recital 136.
[60] 'Deployer' as defined in Article 3(4) and recital 13 of the Artificial Intelligence Act (n 13), is to be interpreted as natural or legal persons *using* an AI system, except for when an AI system is used for strictly personal reasons.
[61] A 'provider' is, according to Article 3(3), a 'natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge'.
[62] ibid Article 50(4).
[63] Cristina Vanberghen, 'The AI Act vs. Deepfakes: A Step Forward, but Is It Enough?' (*Euractiv*, 26 February 2024) <https://www.euractiv.com/section/artificial-intelligence/opinion/the-ai-act-vs-deepfakes-a-step-forward-but-is-it-enough/> accessed 1 September 2025. If a VLOP develops their own AI systems, the obligations of providers would be applicable to it. According to Article 50 and recital 134 in the AI Act a transparency obligation is placed on providers of AI systems, and deployers who manipulate content to 'clearly and distinguishably' disclose that it has been manipulated and is of artificial origin (see the AI Act, recital 134). This includes AI generated text as well, if it aims at informing the public of matters of public interest. But if it has undergone '[…] human review or editorial control and a natural or legal person holds editorial responsibility for the publication of the content' it can be excluded from such demands. This indicates that it is not the actual content, the (dis)information, that is considered in this recital – only whether it was created by an AI, or if a human was involved in the publication process. If VLOPs use such systems embedded into their services, they are to assess them in accordance with Articles 34 and 35 in the DSA (see the AI Act, recital 118).
[64] Digital Services Act (n 12) recital 104.

or lawfulness, or necessarily how widely disinformation is spread, but the *risk* it poses that must be assessed and subsequently mitigated.

Building on this, there are also demands for VLOPs to manage urgent action in times of crisis. In light of Russia's full-scale invasion of and war of aggression against Ukraine in 2022, an article on crisis was added to the DSA in haste.[65] A crisis is defined here as an occurrence '[…] where extraordinary circumstances lead to a serious threat to public security or public health in the Union or in significant parts of it'.[66] If a crisis occurs, and if it is strictly necessary and proportionate, the Commission can demand that VLOPs activate crisis response mechanisms for a limited time, to urgently answer to that specific ongoing crisis.[67] On top of this, in Article 48 DSA, there are provisions encouraging voluntary crisis protocols for addressing crisis situations. The purpose of this would be to rapidly respond to ongoing disinformation campaigns in a coordinated manner.[68]

Still, much is unclear as to the exact demands placed on VLOPs to counter harmful disinformation on their platforms. Due to the open phrasing in articles 34 and 35 of the DSA – enabling platforms to adopt different systems and designs to enforce these requirements – different platforms can choose different focal points in their assessments, or abide by different understandings of, for instance, disinformation.[69] In Article 34 DSA, and the DSA in general, disinformation is not targeted on the basis of its potential illegality, but through its (non-) compliance with a platform's terms and conditions or terms of service.[70] Adapting and adjusting moderation systems, the use of terms of service, and the design and the systems of the platforms, are factors to consider in these risk assessments and mitigations. However, allowing platforms to find best practices benefits flexibility but could also make it more difficult to evaluate the risk assessment regime of VLOPs, to compare and to find a common standard. How much leeway or flexibility is awarded to VLOPs in practice still remains to be seen. The European Commission will, over time, have to clarify whether platforms have effective risk mitigation measures in place for disinformation, and, if not, what exactly is required.

The VLOP 'X' was the first VLOP against which the Commission initiated formal proceedings, only months after the DSA came into force. The European Commission sent requests to X after alleged dissemination of illegal content and disinformation at scale on the platform.[71] The Commission has since opened a formal investigation into several areas of

---

[65] Doris Buijs and Ilaria Buri, 'The DSA's Crisis Approach: Crisis Response Mechanism and Crisis Protocols - DSA Observatory' (*DSA Observatory*, 21 February 2023) <https://dsa-observatory.eu/2023/02/21/the-dsas-crisis-approach-crisis-response-mechanism-and-crisis-protocols/> accessed 1 September 2025.

[66] Digital Services Act (n 12) Article 36(2).

[67] ibid Article 36, recital 91. This first after a recommendation from the European Board's for Digital Services (Article 36(1)).

[68] ibid recitals 91 and 108; Baskaran Balasingham and Sofia Minichová, 'The DSA's Crisis Response Mechanism and the Indispensability of Social Media Networks' (2024) 17(30) Yearbook of Antitrust and Regulatory Studies 127, 129–130; Buijs and Buri (n 65).

[69] Balasingham and Minichová (n 68) 128-130.

[70] João Pedro Quintais, Naomi Appelman, and Ronan Ó Fathaigh, 'Using Terms and Conditions to Apply Fundamental Rights to Content Moderation' (2023) 24(5) German Law Journal 881, 883. Understood in relation to Article 14 in the DSA, stating that VLOPs must take due regard to fundamental rights in their T&Cs, also show the new and groundbreaking way to delegate responsibilities to VLOPs, which in turn, should delegate responsibilities to users by accepting the T&C of the service.

[71] European Commission, 'The Commission Sends Request for Information to X under DSA' (press release, 12 October 2023) <https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4953> accessed 1 September 2025.

content moderation and risk mitigation on the platform. This has not yet been resolved and therefore does not fully clarify the consequences of not moderating disinformation on the platform. The investigation concerns whether X has effective risk mitigation measures in place, such as sufficient moderation resources and adequate moderation systems.[72]

No matter the outcome of such a decision from the Commission, which will add to the understanding of the overarching regulatory measures against disinformation, it is important to recognize the relevance placed on *reach* in relation to risk. Most of the responsibilities imposed on platforms to conduct risk assessment and implement mitigation measures only apply to VLOPs, as in platforms with at least 45 million monthly users. They must comply with the most rigorous rules. This means that other platforms could still have a significant number of users yet not have the same responsibilities to mitigate risks in relation to disinformation. This could indicate a perceived correlation between the reach of certain content and the potential risk for society. The more users that could potentially engage with certain content, the higher the risk.

3.2 PUSHES FOR VOLUNTARY ACTIONS

To guide VLOPs and further clarify their responsibilities, there are explicit references to codes of conduct in the DSA to contribute to its proper application. This is emphasised through Articles 45–47.[73] In recital 104 of the DSA, codes of conduct are mentioned specifically in relation to systemic risks to society and democracy, for example through the dissemination of disinformation. From that same recital it is also clear that 'adherence to and compliance with' a code of conduct by a VLOP could be a suitable mitigating measure for an identified risk and that, if a VLOP refuses to sign or adhere to such a code of conduct, this can be taken into consideration in assessing whether their obligations under the DSA have been met. The importance of VLOPs cooperating is reiterated in both the regulation on the transparency and targeting of political advertising[74] and in the AI Act, which state that VLOPs should adapt AI systems and recommendation systems if needed to mitigate negative effects stemming from personalized recommendations to users. In particular, in order to address problems shared across platforms, VLOPs are expected to join cooperative measures such as codes of conduct.[75]

In other words, directing VLOPs to use codes of conduct for guidance plays a prominent part in the European regulatory framework targeting disinformation. This

---

[72] European Commission, 'Commission Opens Formal Proceedings against X under the DSA' (press release, 18 December 2023) <https://ec.europa.eu/commission/presscorner/detail/en/IP_23_6709> accessed 1 September 2025. There are some preliminary findings available though, on for example the use of dark patterns to mislead users, European Commission, 'Commission sends preliminary findings to X for breach of DSA' (press release, 12 July 2024) <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_3761> accessed 1 September 2025.

[73] However, the use of codes of conduct is mentioned throughout the DSA, in articles as well as recitals, also highlighting their significance in the regulatory framework the DSA provides, see Griffin (n 32) 169

[74] Regulation on the transparency and targeting of political advertising (n 18) recital 20. Here it is stated that '[t]o counter information manipulation and interference in political advertising, "online platforms" as defined in Regulation (EU) 2022/2065 are encouraged, including through the Code of Practice on Disinformation, to establish and implement tailored policies and other relevant measures, including by means of their participation in wider disinformation demonetisation initiatives to prevent the placement of political advertising containing disinformation'.

[75] Artificial Intelligence Act (n 13) recital 88.

approach also allows the Signatories to go beyond the requirements set by the EU by applying their own terms of service. As mentioned, it would be crossing a red line for the Commission to enforce platforms to ban lawful content in their terms of service,[76] but by allowing and encouraging Signatories of codes of conduct to act in certain ways, the responsibilities of VLOPs to act on disinformation become clearer, nonetheless. As mentioned, in early 2025 the European Commission reiterated that 'the Code will become a relevant benchmark for determining DSA compliance regarding disinformation risks'[77] again highlighting its importance. This would also indicate that the Commission gains more influence over how disinformation is interpreted and countered, bypassing the need for detailed regulation.

As previously noted, the Code of Practice on Disinformation adopts a broad definition of the types of content, particularly in certain contexts, that may be classified as disinformation, as well as the actions associated with it, such as foreign or domestic campaigns aimed at interfering with free elections. The question arises, however, as to how Signatories are to perform their duties under the Code and what this will reveal about their obligations under EU regulation to counter lawful disinformation.

Under commitment 14, in the Code of Practice on Disinformation there are several actions and behaviours that Signatories are to target and review, such as ill-intended deepfakes, fake accounts, account takeovers and amplification using bots.[78] In this regard, the transparency obligation for generative AI (deepfakes) under the AI Act is also reiterated for Signatories developing or operating AI-systems and disseminating content on platforms.[79]

It is noteworthy, however, that the first 13 of the 44 commitments relate directly to a single – albeit broad – context: political or issue-based advertising in its various forms. This is a clear focal point of the Code, as very little else, in terms of contexts or types of content, is singled out. The Signatories to the Code[80] commit to reach a common understanding and definition of what 'political and issue advertising' is, which must align with the understanding in the Regulation on the transparency and targeting of political advertising.[81] They also commit to taking actions such as the following: preventing misuse of advertisement systems; clearly indicating if and how advertisement is allowed on their platform; clearly marking content that is sponsored as paid-for content; implementing systems for verification of providers and sponsors of content; and informing users as to why they are seeing certain sponsored political ads.[82] This is directly linked to the risks with disinformation being spread through the use of advertisement. In commitment 13 it is stated that '[r]elevant Signatories agree to engage in ongoing monitoring and research to understand and respond to risks

[76] Husovec, 'The Digital Services Act's Red Line' (n 36).
[77] European Commission, 'The Code of Conduct on Disinformation' (n 20).
[78] European Commission, 'The Strengthened Code of Practice on Disinformation 2022' (n 20) Commitment 14.
[79] Artificial Intelligence Act (n 13) recital 134. See also European Commission, 'The Strengthened Code of Practice on Disinformation 2022' (n 20) Commitment 15.
[80] European Commission, 'Signatories of the 2022 Strengthened Code of Practice on Disinformation' (16 June 2022) <https://digital-strategy.ec.europa.eu/en/library/signatories-2022-strengthened-code-practice-disinformation> accessed 1 September 2025.
[81] European Commission, 'The Strengthened Code of Practice on Disinformation 2022' (n 20) Commitment 4, measure 4.1.
[82] ibid Commitments 2, 6, 7, 8, 9 .

related to Disinformation in political or issue advertising'. For example, the use of 'blackout periods' for political or issue advertisements in relation to elections is to be discussed.

As mentioned in the introductory background to this article, the digital sphere can both enhance the spread and specificity in reach in an efficient way, but beyond these digital developments also give rise to and enable new types of behaviour – such as the creation and amplification of content by non-human actors simulating human interaction. The ever-evolving nature of online communication and manipulation is something that is addressed in the Code of Practice where Signatories are required to recognize novel and evolving disinformation risks in relation to political or issue advertising. This work is intended to be coordinated with other Signatories to the Code of Practice, but also with a *Task-force*, to '*identify novel and evolving disinformation risks*'.[83]

This Task-force is interesting in more ways than one, given that under commitment 37 all Signatories must be part of the permanent Task-force, alongside the European Commission – which chairs the Task-force – representatives from European Regulators Group for Audiovisual Media Services (ERGA), the European Digital Media Observatory (EDMO), and representatives of the European External Action Service (EEAS). Other experts can also be included when needed. The Task-force is mandated to establish more clearly focused methods for risk-assessment to be used in times of crisis or other situations requiring extra structure in order to swiftly respond to risks, such as those surrounding elections. That also includes coordination of actions between platforms. It is also to work to set up and share best practises, for instance on flagging of content as potentially disinformative and creating safe designs of platforms.[84] Such methods and collaborative efforts could further refine the work of VLOPs and other Signatories and help operationalize Articles 34 and 35 of the DSA with its demands for risk assessment and mitigation. It indicates the role of the future Code of conduct on disinformation under the DSA, as a dynamic tool against disinformation.

The Code of Practice and its Signatories also have the potential to increase knowledge on disinformation, for example its progression, contexts, prevalence, and audiences with different levels of resilience, as well as its automated amplification.[85] This should be done by developing structural indicators that are to be evaluated to access the effectiveness of the code going forward.[86] Each Signatory also commits to establishing and maintaining Transparency Centres, with publicly accessible information, including structural indicators, but also other relevant information about how their services work.[87] This can enable both users and other interested parties, such as researchers, to better understand the efforts undertaken to address disinformation and its development.

In the Code of Practice on Disinformation, much of the actual detection of suspicious content is 'delegated' to other parties that are to take some kind of action, other than the

[83] European Commission, 'The Strengthened Code of Practice on Disinformation 2022' (n 20) Commitment 13, measures 13.1 and 13.2.
[84] ibid Commitment 37, measure 37.2.
[85] Iva Nenadić et al, 'Structural Indicators of the Code of Practice on Disinformation: The 2nd EDMO Report' (2024) <https://edmo.eu/wp-content/uploads/2024/03/SIs_-2nd-EDMO-report.pdf > accessed 1 September 2025. See especially pages 6-8.
[86] European Commission, 'The Strengthened Code of Practice on Disinformation 2022' (n 20) IX. Pemanent Task-force, (f), and Commitment 41.
[87] ibid VIII. Transparancy Centre, (a), and Commitments 34 and 35, measure 35.6.

platforms and their moderation systems, namely fact-checkers and the users themselves. Signatories must provide the users with access to functions that enable them to verify the information, such as fact-checking tools where third parties provide verified information or some kind of warning label from reliable sources.[88] The Signatories also commit to cooperate with the fact-checking community, ensuring that such cooperation are solid in terms of funding and neutrality, and when possible, provide them with automated access to information on the platform, as swiftly as possible. This is to guarantee swift and impactful responses from the fact-checkers. Signatories are also required to integrate the findings of fact-checkers on their platform and ensure availability in all languages.[89]

In what must be seen as an important development, in early 2025 Meta changed its policy on disinformation on the platforms Facebook and Instagram, as well as their fact-checking. This shift in Meta's policies is, for now, limited to the United States and nothing is said about challenging the new EU regulations, but it is an interesting development in the approach to disinformation and may indicate something about the need for risk assessments. The spokesperson for the Commission stated that if Meta were to consider such a change in Europe as well, under the DSA a risk assessment submitted to the Commission would be necessary.[90] Considering the strong emphasis on the need for fact-checkers in the Code of Practice on Disinformation, this statement is also noteworthy from that perspective, in terms of the role the Code plays and the strength of certain requirements.

4 CONCLUSIONS: TARGETING 'LAWFUL BUT AWFUL' DISINFORMATION

These concluding remarks aim to summarise and shed light on how the EU targets 'lawful but awful' disinformation by placing responsibilities on VLOPs through these emerging regulatory frameworks. From this study, it is clear that the understanding of what disinformation is and the corresponding demands for VLOPs to counter it are both strongly linked to the assessment and mitigation of risks on platforms. This finding is not in itself all that surprising, given that a focus on platform regulation has been a way for the EU to balance different interests and rights, steering EU policies in general toward risk-based approaches.[91] However, when this is added to how disinformation is discussed in these regulations – as something separate from clearly illegal content – it contributes to a better understanding of when risks will be perceived as having the most harmful impact and the role of VLOPs in countering it.

The definitions of lawful disinformation in these regulations are broad and vague (and often sparse), strengthening the Commission's objective to 'not cross the red line' by censoring specific content on social media platforms. Even so, there is still a clear

[88] European Commission, 'The Code of Conduct on Disinformation' (n 20) Commitments 21 and 22.
[89] European Commission, 'The Strengthened Code of Practice on Disinformation 2022' (n 20) Commitments 30, 31, 32
[90] Cynthia Kroet, 'Meta Needs to Analyse Risks If It Drops Fact Checkers in EU Too' (*euronews*, 8 January 2025) <https://www.euronews.com/next/2025/01/08/meta-needs-to-analyse-risks-if-it-drops-fact-checkers-in-eu-too-commission> accessed 1 September 2025.
[91] Giovanni De Gregorio and Pietro Dunn, 'The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age' (2022) 59(2) Common Market Law Review 473, 475.

relationship between the demands to assess and counter risks and certain content, or rather, *certain contexts*. Free elections and safeguarding democratic processes, broadly speaking, are emphatically and continuously highlighted in these instruments. This regulatory approach by the EU aims to increase transparency for users: clarifying who is behind messages, why they are shown, and whether the message could be false or misleading. This is intertwined with, and sometimes separate from, transparency in advertising.

From this study it is clear that the legal understanding of risk, as opposed to the intent of actors, is the driving factor behind these responsibilities placed on VLOPs. The intent of actors (state, groups/individuals) is not as relevant as the societal and democratic risk of certain actions in certain contexts. The role of social media platforms and their reach in society is contextually bound to the risk of certain content and actions on platforms – especially on VLOPs.

Another indication of this is the intended role of VLOPs as quasi-collaborators – or perhaps even spokespersons – for the European Commission during times of crisis. The crisis response mechanism in Article 36 of the DSA is a good example of both the understanding of, and intended role for, VLOPs under these emerging frameworks. Not only does the potential to cause harm on major platforms serve as proof of their prominent role, but so does the possibilities of using them to quickly disseminate reliable information. However, this is also a way for the Commission to rapidly reach the public with information it deems important during times of crisis, giving the Commission significant scope to intervene in the moderation process of VLOPs. Though this is only for a limited time (a maximum of three months),[92] it can provide the Commission with a substantial power to seek control of the dissemination of certain content.[93] This has also been criticised because of its implications for freedom of expression.[94] The crisis response mechanism was initially intended as a voluntary measure,[95] however, it has since become evident that the Commission considered the risks posed by the widespread dissemination of disinformation or illegal content during crises sufficiently serious to warrant removing such discretion from platforms.

The fact that VLOPs are clearly singled out in terms of obligations under these regulatory instruments also indicates a perceived relationship between risk and *reach*, as mentioned. The more users that could potentially engage with certain content, the higher the risk for society. However, the dissemination of disinformation across smaller platforms or communities could still cause harm, for example, through radicalisation among conspiracy theorists.[96] To some extent the risks posed on smaller platforms or forums could indirectly be said to be addressed in the DSA through provisions encouraging self- and co-regulatory instruments between and across platforms of different sizes in order to cooperate and

[92] Digital Services Act (n 12) Article 36(3)(c).
[93] Ronan Fahy, Naomi Appelman, and Natali Helberger, 'The EU's Regulatory Push against Disinformation' (*Verfassungsblog*, 5 August 2022) <https://verfassungsblog.de/voluntary-disinfo/> accessed 1 September 2025.
[94] European Digital Rights, 'Public Statement On New Crisis Response Mechanism and Other Last Minute Changes to the DSA' (EDRi, 12 April 2022) <https://edri.org/wp-content/uploads/2022/04/EDRi-statement-on-CRM.pdf> accessed 1 September 2025.
[95] Jörg Frederik Ferreau, 'Crisis? What Crisis? The Risk of Fighting Disinformation with the DSA's Crisis Response Mechanism' (2024) 16(1) Journal of Media Law 57, 58.
[96] McGonagle and Pentney (n 23) 49.

develop best practices.[97] That being said, it is reasonable to impose obligations based on platform size due to VLOPs' dominant positions and reach, as well as the need for financial resources and a well-functioning, adaptable infrastructure. This focus on VLOPs can nevertheless leave blind spots for the dissemination of disinformation.[98]

The efforts to encourage adherence to the Code of Conduct on disinformation are relevant to understanding how VLOPs and other signatories are expected to combat disinformation and, in particular, to understanding how they are supposed to work with assessing and mitigating risk. The DSA does not provide clear guidance as to the specifics of the methodology for this, which also makes the assessment of VLOPs' adherence to the demands difficult and hinders comparisons between platforms. The work of the Task-force to establish more clearly focused methods for risk-assessment could prove useful in structuring the work of VLOPs in line with regulatory demands.

Because the Code of Practice has now become a code of conduct under the DSA, more VLOPs can be expected to join as a way to fulfil their obligations. However, the many explicit efforts to encourage participation in codes of conduct would still not – in themselves – provide much incentive for compliance, since there are no sanctions for non-compliance.[99] With that being said, the VLOP 'X' left the code in 2023, prompting warnings from the Commission that the rules under the DSA still must be followed.[100] Nevertheless, complying with a code of conduct is an indication of compliance with the mentioned demands for risk assessment and risk mitigation, and non-compliance with risk assessment obligations can result in significant fines under Article 74. At the same time, participating and joining a code of conduct does not assure compliance with the DSA,[101] but is surely the strongest indicator for VLOPs of what actions are needed.

Taken together, the demands stated in the Code of Practice on Disinformation are far more precise than those found in the DSA, the AI Act and the Regulation on the Transparency and Targeting of Political Advertising. The Code builds on all three instruments, reiterating the risks of political interference through the use of fake accounts, bots and deepfakes, while highlighting the need for transparency so as to provide users with insight into who is behind an account or message. In addition, Signatories are subject to continuous reporting obligations concerning the policies and routines they apply, as well as the actions they take to moderate and detect content, thereby allowing insight into their ongoing work against disinformation.

How the Code of Practice, now a formal code of conduct under the DSA, is put into action and enforced will have a significant impact on targeting disinformation that does not, in itself, fall into the category of illegal content. This could provide greater clarity regarding the Signatories' compliance with emerging regulatory instruments. In turn, it may contribute

---

[97] Digital Services Act (n 12) recital 88.
[98] This is also discussed in McGonagle and Pentney (n 23) 49.
[99] Jaursch (n 42); Julian Jaursch, 'What Can DSA Codes of Conduct for Online Advertising Achieve?' (*Interface*, 16 December 2024) <https://www.interface-eu.org/publications/dsa-advertising-codes> accessed 1 September 2025.
[100] Lisa O'Carroll, 'EU Warns Elon Musk after Twitter Found to Have Highest Rate of Disinformation' (*The Guardian*, 26 September 2023) <https://www.theguardian.com/technology/2023/sep/26/eu-warns-elon-musk-that-twitter-x-must-comply-with-fake-news-laws> accessed 1 September 2025.
[101] See Cynthia Kroet, 'Online Platforms Disinformation Code Going Formal, but X Is Out' (*euronews*, 13 February 2025) <https://www.euronews.com/next/2025/02/13/online-platforms-disinformation-code-going-formal-but-x-is-out> accessed 1 September 2025.

to a better understanding of how 'lawful but awful' disinformation should be addressed and help to clarify the role of VLOPs in this regard. Or in the words of Mündges and Park:

> This will be particularly significant when the Code of Practice transitions into a code of conduct under the DSA. As it is likely to be the first one, the way this transition is managed, its impact, and its implementation by regulators and policymakers will largely determine the DSA's effectiveness in regulating harmful but mostly lawful speech.[102]

This will not only demonstrate the DSA's effectiveness but also the influence of the Commission on 'lawful but awful' disinformation. The focus on risk and the need for VLOPs to demonstrate risk mitigation measures are tied to voluntary codes where the Commission holds significant influence. This at least presents the possibility that the Commission may move increasingly toward a more specific focus on content, without formally legislating. This will perhaps not cross, but rather blur, the red line through soft law instruments and compliance mechanisms.

[102] Stephan Mündges and Kirsty Park, 'But Did They Really? Platforms' Compliance with the Code of Practice on Disinformation in Review' (2024) 13(3) Internet Policy Review, 16 <https://policyreview.info/articles/analysis/platforms-compliance-code-of-practice-on-disinformation-review> accessed 1 September 2025.

LIST OF REFERENCES

Balasingham B and Minichová S, 'The DSA's Crisis Response Mechanism and the Indispensability of Social Media Networks' (2024) 17(30) Yearbook of Antitrust and Regulatory Studies 127
DOI: https://doi.org/10.7172/1689-9024.yars.2024.17.30.5

Benjamin Farrand, 'Regulating Misleading Political Advertising on Online Platforms: An Example of Regulatory Mercantilism in Digital Policy' (2024) 45(5) Policy Studies 730
DOI: https://doi.org/10.1080/01442872.2023.2258810

Chander A, 'When the Digital Services Act Goes Global' (2023) 38(4) Berkeley Technology Law Review 1067
DOI: https://doi.org/10.15779/Z38RX93F48

De Blasio E and Selva D, 'Who Is Responsible for Disinformation? European Approaches to Social Platforms' Accountability in the Post-Truth Era' (2021) 65(6) American Behavioral Scientist 825
DOI: https://doi.org/10.1177/0002764221989784

De Gregorio G and Dunn P, 'The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age' (2022) 59(2) Common Market Law Review 473
DOI: https://doi.org/10.54648/cola2022032

De Gregorio G and Pollicino O, 'The European Approach to Disinformation: Policy Perspectives' (Institute for European Policymaking, June 2024) <https://iep.unibocconi.eu/sites/default/files/media/attach/PB19_Disinformation_%20Pollicino.pdf> accessed 1 September 2025

Diaz Ruiz C and Nilsson T, 'Disinformation and Echo Chambers: How Disinformation Circulates on Social Media Through Identity-Driven Controversies' (2023) 42(1) Journal of Public Policy & Marketing 18
DOI: https://doi.org/10.1177/07439156221103852

Enarsson T, 'Navigating Hate Speech and Content Moderation under the DSA: Insights from ECtHR Case Law' (2024) 33(3) Information & Communications Technology Law 384
DOI: https://doi.org/10.1080/13600834.2024.2395579

Enarsson T, Enqvist L, and Naarttijärvi M, 'Approaching the Human in the Loop – Legal Perspectives on Hybrid Human/Algorithmic Decision-Making in Three Contexts' (2022) 31(1) Information & Communications Technology Law 123
DOI: https://doi.org/10.1080/13600834.2021.1958860

Ferreau JF, 'Crisis? What Crisis? The Risk of Fighting Disinformation with the DSA's Crisis Response Mechanism' (2024) 16(1) Journal of Media Law 57
DOI: https://doi.org/10.1080/17577632.2024.2362481

Galantino S, 'How Will the EU Digital Services Act Affect the Regulation of Disinformation?' (2023) 20(1) SCRIPTed 89

Griffin R, 'Codes of Conduct in the Digital Services Act: Functions, Benefits & Concerns' (2024) 2024 Technology and Regulation 167

Howard PN and Kollanyi B, 'Bots, #Strongerin, and #Brexit: Computational Propaganda During the UK-EU Referendum' (*SSRN*, 20 June 2016), 5 <https://papers.ssrn.com/abstract=2798311> accessed 1 September 2025
DOI: https://doi.org/10.2139/ssrn.2798311

Husovec M, 'Rising Above Liability: The Digital Services Act as a Blueprint for the Second Generation of Global Internet Rules' (2023) 38(3) Berkeley Technology Law Journal 884
DOI: https://doi.org/10.15779/Z38M902431

——, 'The Digital Services Act's Red Line: What the Commission Can and Cannot Do about Disinformation' (2024) 16(1) Journal of Media Law 47
DOI: https://doi.org/10.1080/17577632.2024.2362483

Kozyreva A et al, 'Resolving Content Moderation Dilemmas between Free Speech and Harmful Misinformation' (2023) 120(7) Proceedings of the National Academy of Sciences e2210666120
DOI: https://doi.org/10.1073/pnas.2210666120

Łabuz M, 'Regulating Deep Fakes in the Artificial Intelligence Act' (2023) 2(1) Applied Cybersecurity & Internet Governance 1
DOI: https://doi.org/10.60097/acig/162856

Lewis B, 'Rabbit Hole: Creating the Concept of Algorithmic Radicalization' in Farkas J and Maloney M (eds) *Digital Media Metaphors* (Routledge 2024)
DOI: https://doi.org/10.4324/9781032674612-10

Mbioh W, 'Beyond Echo Chambers and Rabbit Holes: Algorithmic Drifts and the Limits of the Online Safety Act, Digital Services Act, and AI Act' (2024) 33(3) Griffith Law Review 189
DOI: https://doi.org/10.1080/10383441.2025.2481544

McGonagle T and Pentney K, 'From Risk to Reward? The DSA's Risk-Based Approach to Disinformation' in Capello M et al (eds), *Unravelling the Digital Services Act package* (European Audiovisual Observatory 2021)

Mündges S and Park K, 'But Did They Really? Platforms' Compliance with the Code of Practice on Disinformation in Review' (2024) 13(3) Internet Policy Review <https://policyreview.info/articles/analysis/platforms-compliance-code-of-practice-on-disinformation-review> accessed 1 September 2025
DOI: https://doi.org/10.14763/2024.3.1786

Nenadić I et al, 'Structural Indicators of the Code of Practice on Disinformation: The 2nd EDMO Report' (2024) <https://edmo.eu/wp-content/uploads/2024/03/SIs_-2nd-EDMO-report.pdf > accessed 1 September 2025

Nikiforov L, 'Transparency in Targeting of Political Advertising: Challenges Remain' (*SSRN*, 1 November 2024) <https://papers.ssrn.com/abstract=5054430> accessed 1 September 2025
DOI: https://doi.org/10.2139/ssrn.5054430

Ó Fathaigh R, Helberger N, and Appelman N, 'The Perils of Legally Defining Disinformation' (2021) 10(4) Internet Policy Review <https://policyreview.info/articles/analysis/perils-legally-defining-disinformation> accessed 1 September 2025
DOI: https://doi.org/10.14763/2021.4.1584

Pariser E, *The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think* (Penguin Books Ltd 2011)

Peck A, 'A Problem of Amplification: Folklore and Fake News in the Age of Social Media' (2020) 133(529) Journal of American Folklore 329
DOI: https://doi.org/10.5406/jamerfolk.133.529.0329

Porter T and Ronit K, 'Self-Regulation as Policy Process: The Multiple and Criss-Crossing Stages of Private Rule-Making' (2006) 39 Policy Sciences 41
DOI: https://doi.org/10.1007/s11077-006-9008-5

Quintais JP, Appelman N, and Ó Fathaigh R, 'Using Terms and Conditions to Apply Fundamental Rights to Content Moderation' (2023) 24(5) German Law Journal 881
DOI: https://doi.org/10.31219/osf.io/f2n7m

Rauchegger C and Kuczerawy A, 'Injunctions to Remove Illegal Online Content under the Ecommerce Directive: Glawischnig-Piesczek' (*SSRN*, 31 August 2020) <https://papers.ssrn.com/abstract=3728597> accessed 1 September 2025
DOI: https://doi.org/10.2139/ssrn.3728597

Rojszczak M, 'The Digital Services Act and the Problem of Preventive Blocking of (Clearly) Illegal Content' (2023) 3(2) Institutiones Administrationis – Journal of Administrative Sciences 44
DOI: https://doi.org/10.54201/iajas.v3i2.85

Shattock E, 'Fake News in Strasbourg: Electoral Disinformation and Freedom of Expression in the European Court of Human Rights (ECtHR)' (2022) 13(1) European Journal of Law and Technology 1

Steinert S and Dennis MJ, 'Emotions and Digital Well-Being: On Social Media's Emotional Affordances' (2022) 35 Philosophy & Technology 36
DOI: https://doi.org/10.1007/s13347-022-00530-6

Vander Maelen C, 'Hardly Law or Hard Law? Investigating the Dimensions of Functionality and Legalisation of Codes of Conduct in Recent EU Legislation and the Normative Repercussions Thereof' (2022) 47(6) European Law Review 752

VARIETIES OF AN EFFECTS-BASED APPROACH TO ABUSE OF DOMINANCE: UNDERSTANDING THE TWO CONCEPTS OF PRESUMPTIONS IN THE EU COMMISSION'S DRAFT GUIDELINES ON EXCLUSIONARY ABUSES

SIMON DE RIDDER*

Following severe dysfunctionalities in the enforcement of Article 102 TFEU and major setbacks in the judicial review of its prohibition decisions, the European Commission has drafted Guidelines on exclusionary abuses that entail two distinct concepts of presumptions to ease the burden borne by the Commission when proving that a dominant undertaking's allegedly abusive conduct is capable of producing exclusionary effects. These presumptions do not abandon an effects-based approach to abuse of dominance. Rather, they fit into the everlasting struggle of finding an adequate evidentiary law standard to show potential exclusionary effects and, in principle, are very much consistent with the Union Courts' recent jurisprudence on Article 102 TFEU. The tests triggering the presumptions might, however, need additional refinement in the process to adopt the Guidelines, or in the Commission's future decision-making practice, and so their practical value is yet to be determined.

1 INTRODUCTION

The public enforcement of Article 102 TFEU has faced significant challenges in the last decade. In cases before the European Commission, proceedings have sometimes lasted up to six, eight or even ten years.[1] This is undoubtedly the result of a multitude of factors, some of which relate to the peculiarities of procedural law in proceedings before the Commission under Regulation 1/2003.[2] Another factor, which stems from the Commission itself, has long been recognized as an obstacle to effective enforcement: since the 2000s, the Commission's so-called 'more economic' approach to abuse of dominance, particularly reflected in its 2009 Priorities Guidance,[3] emphasized the importance of accurately assessing

* Research Assistant and PhD Candidate; Faculty of Law, Humboldt-Universität zu Berlin. Email: simon.eric.deridder@googlemail.com.
For valuable comments and discussion, I am grateful to Björn Becker, Elias Deutscher, Lennart Enwaldt, David Fåhraeus, Johannes Holzwarth, Philipp Hornung, Robert Welker, and Maximilian Wolters, as well as the participants of the 2025 BECCLE conference and the Competition Law Research Colloquium at Humboldt-Universität zu Berlin. All opinions and mistakes remain my own.
[1] See for a comprehensive study, Heike Schweitzer and Simon de Ridder, 'How to Fix a Failing Art. 102 TFEU' (2024) 15(4) Journal of European Competition Law & Practice 222, 223-227.
[2] Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty [2003] OJ L1/1 (Regulation 1/2003). These procedural rules are currently under evaluation by the Commission, see Massimiliano Kadar, 'Evaluating 20 Years of Regulation 1/2003: Are EU Antitrust Procedures "Fit for the Digital Age"?' (2024) 85(3) Antitrust Law Journal 577.
[3] Communication from the Commission – Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings [2009] OJ C45/7 (2009 Priorities Guidance).

the exclusionary effects of a dominant undertaking's conduct in each individual case in order to avoid false positives in public enforcement. Combined with case law that appears to be increasingly in flux, this could have significant consequences: if a prohibition decision comes a decade, or even half a decade, too late, it can usually no longer remedy the damage to competition already caused by the anti-competitive conduct.[4] In this respect, there is essentially no difference between a false negative and a correct prohibition decision that is issued too late.[5] Furthermore, Article 102 TFEU is at risk of losing its deterrent effect. This is even more true in highly dynamic, especially digital, sectors.

Against this backdrop, the Commission has started its attempt to refine the enforcement of Article 102 TFEU with the key concern of removing obstacles to public enforcement. Its plan to adopt Guidelines on exclusionary abuses in the course of 2025 aims at developing a 'workable effects-based approach to abuse of dominance'.[6] This is now also enshrined in the introduction to the Commission's draft for such Guidelines, which states that 'it is important that Article 102 TFEU is applied vigorously and effectively'.[7] In attempting to achieve this, the Draft Guidelines, in some respects, tend to deviate significantly from the 2009 Priorities Guidance and the Commission's subsequent decision-making practice. Notably, the Draft Guidelines rely on 'general principles' of abuse of dominance by providing a two-pillar test for finding an abuse.[8] In that, apart from a conduct's effects on competition,[9] the deviation of such conduct from the concept of 'competition on the merits' gains considerable weight compared to the Commission's previous decisional practice.[10] Another bold choice by the Commission is to establish a system of presumptions

[4] Schweitzer and de Ridder (n 1) 223.
[5] ibid 225.
[6] Linsey McCallum et al, 'A dynamic and workable effects-based approach to abuse of dominance' (Competition Policy Brief No 1/2023) <https://op.europa.eu/en/publication-detail/-/publication/ef8f0a39-cf77-11ed-a05c-01aa75ed71a1/language-en> accessed 1 September 2025.
[7] Draft for a Communication from the Commission – Guidelines on the application of Article 102 of the Treaty on the Functioning of the European Union to abusive exclusionary conduct by dominant undertakings <https://competition-policy.ec.europa.eu/public-consultations/2024-article-102-guidelines_en> accessed 1 September 2025 ('Draft Guidelines'), para 4.
[8] Especially: Draft Guidelines (n 7) para 45.
[9] The insufficiency of an effects criterion alone to distinguish normal competitive behaviour from abuses of dominance has been acknowledged since the earliest days of modern European competition law, see Ernst-Joachim Mestmäcker, *Das marktbeherrschende Unternehmen im Recht der Wettbewerbsbeschränkungen* (Mohr Siebeck 1959) 17: 'Neither the effect nor the means of competitive conduct suffice in and of themselves to separate the exercise of free competition from the exercise of market power. The particular difficulties law faces in assessing market behaviour originate in the fact that every undertaking exerts power as soon as it operates on the market'. (Original German: 'Aber weder die Wirkung […] noch das Mittel […] einer Wettbewerbshandlung reichen für sich allein aus, um […] die Ausübung freien Wettbewerbs von der Ausübung von Marktmacht zu trennen. Die besonderen Schwierigkeiten, die dem Recht […] bei der Beurteilung des Marktverhaltens begegnen, gehen darauf zurück, daß jedes Unternehmen seine Macht ausübt, sobald es auf dem Markt tätig wird').
[10] This has, despite being firmly grounded in the Union Courts' case law on what constitutes an abuse under Article 102 TFEU, sparked considerable criticism, see generally Pınar Akman, 'A Critical Inquiry into "Abuse" in EU Competition Law' (2024) 44(2) Oxford Journal of Legal Studies 405, 412; Chiara Fumagalli and Massimo Motta, 'Economic Principles for the Enforcement of Abuse of Dominance Provisions' (2024) 20(1-2) Journal of Competition Law & Economics 85, 90-92. For criticism with a view specific to the Draft Guidelines, see Pınar Akman, Chiara Fumagalli, and Massimo Motta, 'The European Commission's draft guidelines on exclusionary abuses: a law and economics critique and recommendations' [2025] Journal of European Competition Law & Practice, 4 <https://doi.org/10.1093/jeclap/lpaf020> accessed 1 September 2025; Assimakis Komninos, 'The European Commission's Draft Guidelines on Exclusionary Abuses – A

to assess whether conduct is capable of producing exclusionary effects.[11] This overturns the Commission's previous self-commitment, as part of its 'more economic' approach, to assess foreclosure effects individually on a case-by-case basis.[12]

In doing so, the Commission takes the next step in what appears to be an everlasting struggle of the law on abuse of dominance:[13] Finding an evidentiary law framework for the analysis of effects on competition that properly balances, on one hand, the desire to base decision on up-to-date economic insight and the right to be heard of the dominant undertakings, and on the other, the public interest in a functioning (and deterring) public enforcement of the competition rules and legal certainty on the other hand. Being a less than profound insight, an effects-based approach by no means presupposes that the enforcement of Article 102 TFEU focuses solely on achieving the most correct analysis of effects and avoiding false positives, nor that a case-by-case economic analysis of exclusionary effects is the sole legal standard to finding an abuse.[14] In fact, EU competition law has brought forth different varieties of an effects-based approach to abuse of dominance throughout its history, all of which strike the difficult balance slightly differently. In this article, I intend to show that the case law of the Union Courts in principle supports the establishment of presumptions as part of such an effects-based approach to the notion of abuse under Article 102 TFEU. While bearing the case law in mind, I will examine the two concepts of presumptions, their underlying rationale, their functioning and the respective tests for triggering the presumption, which will show that notable ambiguity remains regarding the relevant tests. Whether the presumptions will live up to the expectations set for them remains an open question.

2 VARIETIES OF AN EFFECTS-BASED APPROACH TO ABUSE OF DOMINANCE

The mere fact that the Commission recognises presumptions of exclusionary effects in no way implies the abandonment of an effects-based approach to abuse of dominance. Since the Court of Justice's judgment in *Hoffmann-La Roche*, an exclusionary abuse has been defined

Very Selective Restatement of the Case Law' (*EU Law Live's Competition Corner*, 14 November 2024) <https://eulawlive.com/competition-corner/op-ed-the-european-commissions-draft-guidelines-on-exclusionary-abuses-a-very-selective-restatement-of-the-case-law/> accessed 1 September 2025; Damien J Neven, 'Competition on the Merits?' (*EU Law Live's Competition Corner*, 30 October 2024) <https://eulawlive.com/competition-corner/competition-on-the-merits-by-damien-j-neven/> accessed 1 September 2025.

[11] Namely in the Draft Guidelines (n 7) para 60. For the fact that the substantive legal test is the 'capability' of a conduct to produce effects, see Draft Guidelines (n 7) para 61; Schweitzer and de Ridder (n 1) 230-231; exemplary from the case law: Case C-377/20 *Servizio Elettrico Nazionale and Others* EU:C:2022:379 para 50.

[12] See below Section 2.2. This has also been positively highlighted by the German Federal Ministry of Economic Affairs and Climate Action in its 'Contribution to the Commission's consultation on the draft Guidelines on exclusionary abuses of dominance', 2 <https://competition-policy.ec.europa.eu/public-consultations/2024-article-102-guidelines_en> accessed 1 September 2025.

[13] And EU competition law altogether, looking at the ongoing discussion on delineating 'by object' and 'by effect' restrictions under Article 101 TFEU. Both of these discussions may of course learn from each other, especially given the apparently increased significance of a somewhat 'consistent interpretation' of the competition rules, see Case C-606/23 *Tallinna Kaubamaja and KIA Auto* EU:C:2024:1004 paras 35-36; Case C-333/21 *European Superleague Company* EU:C:2023:1011 para 186.

[14] Even the fiercest critics of the Draft Guidelines' presumptions usually do not resent the idea of presumptions altogether, see Akman, Fumagalli, and Motta (n 10) 9; Komninos, 'The European Commission's Draft Guidelines on Exclusionary Abuses' (n 10).

as conduct which 'through recourse to methods different from those which condition normal competition […], has the effect of hindering the maintenance of the degree of competition still existing in the market or the growth of that competition'.[15] Given this general definition, which has since been constantly confirmed in the Union Courts' case law,[16] any approach to abuse of dominance must take into account the relevant conduct's effect on competition.[17] There are, however, different varieties of this effects-based approach. In the following discussion, I will conceptualize three such varieties.[18]

2.1 VARIETY 1: *HOFFMANN-LA ROCHE*'S CONDUCT-BASED PRESUMPTIONS

The judgment in *Hoffmann-La Roche* is in many ways illustrative of the approach taken by the Courts in the early days of Community competition law: The Commission found that Hoffmann-La Roche had abused its dominant position through agreements that either directly obliged purchasers to buy all their requirements exclusively, or in preference, from Hoffmann-La Roche, or did so indirectly by offering purchasers incentives in the form of fidelity rebates.[19] The Court of Justice upheld the Commission's decision finding that exclusivity agreements and fidelity rebates were indeed abusive.[20] In ruling these types of practices abusive, the Court actively assessed the potential effects they would have on competition: any obligation or incentive for a purchaser to obtain their supplies exclusively from the dominant undertaking would, in the first place, deprive the purchaser of their choice of sources of supply and, in the second place, deny other producers access to the market; this would, of course, consolidate the dominant undertaking's position in the market.[21] Considering fidelity rebates, the Court held that their effects were comparable to those of exclusivity agreements, because, unlike quantity rebates, they were incentivising purchasers to purchase exclusively from the dominant undertaking. Additionally, the Court considered the fidelity rebates to be discriminatory.

Though this has been widely criticized as 'formalistic',[22] the Court's finding was in fact based on an assessment of the possibility that the conduct had exclusionary effects – even if only on an abstract level[23] – and, in doing so, effects-based of sorts. However, the capability to produce effects was presumed for certain types of conduct, and this presumption was irrebuttable. The dominant undertaking in question would not be able to bring forward evidence that, in the circumstances of the individual case, its conduct was not capable of

---

15 Case 85/76 *Hoffmann-La Roche v Commission* EU:C:1979:36 para 91.
16 See for example from the last years: *Servizio Elettrico Nazionale* (n 11) para 44; *European Superleague* (n 13) para 125; Case C-48/22 P *Google and Alphabet v Commission (Google Shopping)* EU:C:2024:726 para 88; Case C-240/22 P *Commission v Intel Corporation (Intel II)* EU:C:2024:915 para 176.
17 For the fact that the effects the allegedly abusive conduct has on competition always and constantly played a role, see the examples from Raffaele Di Giovanni Bezzi, 'A Tale of Two Cities: Effects Analysis in Article 102 TFEU Between Competition Process and Market Outcome' (2023) 14(2) Journal of European Competition Law & Practice 83, 84-86.
18 The granularity of this differentiation is rather arbitrary. Importantly, they show that the case law resembles shades of grey rather than a black and white picture.
19 *Vitamins* (Case IV/29.020) Commission Decision 76/642/EEC [1976] OJ L223/27.
20 *Hoffmann-La Roche* (n 15) para 89.
21 See, here and in the following, *Hoffmann-La Roche* (n 15) para 90.
22 See Akman (n 10) 411-412 with further references.
23 Nada Ina Pauer, 'From Intel & Qualcomm to the new Art. 102 TFEU-Guidelines' (2024) 22(2) Zeitschrift für Wettbewerbsrecht 115, 123.

producing exclusionary effects. Rather, once the Commission or the Courts found a type of conduct that was abusive, the dominant undertaking could only rely on an objective justification or an efficiency defence. This type of irrebuttable presumption – even if considered 'formalistic' – provided the undertakings concerned with a high degree of certainty and was arguably based on implicit assumptions on the level of risk competition law should accept regarding harm to competition.[24]

2.2 VARIETY 2: THE COMMISSION'S 'MORE ECONOMIC' APPROACH

In the late 2000s, as part of its so-called 'more economic' approach to abuse of dominance, the Commission committed itself to a detailed analysis of a conduct's effects on competition in each individual case, laying out this rationale in its 2009 Priorities Guidance: '[t]he Commission will normally intervene under Article 82 [now: Article 102 TFEU] where, on the basis of cogent and convincing evidence, the allegedly abusive conduct is likely to lead to anti-competitive foreclosure'.[25] In an attempt to avoid false positives, making the precision of the economic assessment the primary objective of its enforcement policy, the Commission left no room for any shortcuts in the assessment of exclusionary effects.[26]

The Commission did, of course, not fulfil all the promises of the 'more economic' approach in its subsequent decisional practice. In particular, the Commission quickly abandoned attempts to directly prove consumer harm,[27] but the effects analysis remained an important part of Commission decisions in abuse of dominance cases without recourse to analytical shortcuts, such as presumptions. The Commission first used this approach in its landmark *Intel* decision, which shows its departure from the principles of *Hoffmann-La Roche* – fittingly, a case on rebates as well. The Commission investigated rebates that Intel had granted different Original Equipment Manufacturers (OEMs) upon exclusivity regarding its x86 Central Processing Units (CPUs). The Commission carried out an 'as efficient competitor test', by first calculating the 'required share', i.e. the market share an entrant must obtain to compete against the incumbent, and subsequently comparing this against the 'contestable share', i.e. the share of a customer's purchase requirements that can realistically be switched to a new supplier in a given time.[28] As in each case the contestable share was below the required one, the Commission found Intel's rebates capable of

[24] Schweitzer and de Ridder (n 1) 237. To that respect, it is important to bear in mind that Article 102 TFEU by no means requires a finding of actual effects on competition. It rather reacts to the risk of distortions of competition that some conduct comes with, see *Servizio Elettrico Nazionale* (n 11) para 53; Case C-680/20 *Unilever Italia Mkt. Operations* EU:C:2023:33 para 41.

[25] 2009 Priorities Guidance (n 3) para 20.

[26] According to para 22 of the 2009 Priorities Guidance (n 3), only in cases where 'conduct can only raise obstacles to competition' or 'creates no efficiencies', the Commission would not be required to carry out a detailed assessment of effects.

[27] Tristan Rohner, *Art. 102 AEUV und die Rolle der Ökonomie* (Nomos 2023) 220; for an example see Schweitzer and de Ridder (n 1) 226 in fn 26.

[28] *Intel* (Case COMP/C-3/37.990) Commission Decision of 13 May 2009, recitals 1002-1576. For the 'as efficient competitor test' in general, see Adriano Barbera, Nicolás Fajardo Acosta, Timo Klein, 'The Role of the AEC Principle and Test in a Dynamic and Workable Effects-Based Approach to Abuse of Dominance' (2023) 14(8) Journal of European Competition Law & Practice 582; Damien J Neven, 'The As-Efficient Competitor Test and Principle' (2023) 14(8) Journal of European Competition Law & Practice 565; Renato Nazzini, *The Foundations of European Union Competition Law* (Oxford University Press 2011) ch 7; for the 'as efficient competitor test' in *Intel*, see Robert Lauer, 'The Intel saga: what went wrong with the Commission's AEC test (in the General Court's view)?' (2024) 20(1) European Competition Journal 45.

foreclosing equally efficient competitors.[29]

The 'as efficient competitor test' widely serves as a symbol of the increased complexity in the Commission's economic assessment, but even apart from this test, the Commission would, too, go beyond the requirements of the older case law, as its decision in *Qualcomm (Exclusivity payments)* illustrates.[30] The dominant undertaking, Qualcomm, granted Apple payments under the condition that Apple obtained all its demand for LTE chipsets from Qualcomm, which the Commission considered to be exclusivity agreements.[31] As shown above, this finding alone would have been sufficient under the *Hoffmann-La Roche* doctrine for the Commission to conclude that Qualcomm's conduct could have exclusionary effects. However, the Commission, in its decision, went on to fully analyse the potential of Qualcomm's payments to exert such effects, using quantitative and qualitative evidence, by showing that these payments reduced Apple's incentives to switch to competing LTE chipset suppliers[32] and covered a significant share of the market for LTE chipsets in the period concerned,[33] and that Apple was an attractive customer to LTE chipset suppliers considering its importance for entry and expansion in the global market for LTE chipsets.[34] As opposed to the approach taken by the Court of Justice in *Hoffmann-La Roche*, the Commission's 'more economic' approach no longer regarded the potential exclusionary effects relevant on an abstract level, but instead required it to actually examine the specific capability of the dominant undertaking's conduct to exert effects in each individual case.

2.3 VARIETY 3: THE UNION COURTS' RECENT CASE LAW

The Court of Justice's more recent case law brought forth a third variety of an effects-based approach, located somewhere between *Hoffmann-La Roche*'s conduct-based presumptions and the Commission's self-commitment to assess effects individually in each case. The story of this third variety begins 6 September 2017, when the Court of Justice, supposedly in an attempt to 'clarify' the older case law,[35] significantly modified *Hoffmann-La Roche*'s presumption regarding rebate schemes in its first judgment in the *Intel* saga. Intel had argued that the finding of the capability to exert effects would require 'an examination of all the circumstances, including the level of the rebates in question, their duration, the market shares concerned, the needs of customers and the capability of the rebates to foreclose an as efficient competitor'.[36] Against this background, the Court of Justice held that if the dominant undertaking submits during the administrative procedure, and on the basis of supporting evidence, that its conduct was not capable of restricting competition, the

[29] See Commission Decision in *Intel* (n 28) recitals 1154, 1281, 1406, 1456, 1507, 1573. While the Commission stated in the decision that it was not obligated to carry out an 'as efficient competitor test' (recital 925), this test ultimately was the Commission's main source of finding the alleged foreclosure, see Rohner (n 27) 118.
[30] On the Commission's assessment in this case, see also Massimiliano Kadar, 'Article 102 and Exclusivity Rebates in a Post-Intel World' (2019) 10(7) Journal of European Competition Law & Practice 439, 444-445.
[31] *Qualcomm (Exclusivity payments)* (Case AT.40220) Commission Decision of 24 January 2018, recitals 395-400.
[32] ibid recitals 412-465.
[33] ibid recitals 466-473.
[34] ibid recitals 474-485.
[35] Case C-413/14 P *Intel v Commission (Intel I)* EU:C:2017:632 para 138. In fact, the Court of Justice 'dresses up change as continuity', see Elias Deutscher, 'Causation and counterfactual analysis in abuse of dominance cases' (2023) 19(3) European Competition Journal 481, 517.
[36] See *Intel I* (n 35) para 111.

Commission could no longer rely on the *Hoffmann-La Roche* presumption; rather, the Commission would then have to analyse, inter alia, the extent of the dominant position, the share of the market affected, the duration of the conduct in question and the possible existence of a strategy aiming to exclude competitors.[37] The Court of Justice did not flat out abandon the concept of presumptions, but it did however change their functioning. Now, the dominant undertaking would only have to submit (supported by evidence) that its conduct was not in fact capable of producing the alleged effect in order for the Commission to be obliged to investigate again.

What initially might have looked like a development specific to rebate schemes turned out to be a larger trend. Since *Intel*, the Union Courts have clarified and further specified this case law in a series of judgments. Now, as a general rule, when a dominant undertaking submits, during the administrative procedure and with supporting evidence, that its conduct was not capable of producing exclusionary effects, the Commission[38] is required to examine whether, in the circumstances of case, the conduct in question was indeed capable to do so.[39] The Commission must, then, pay due attention to the arguments submitted by the dominant undertaking, and examine carefully and impartially all the relevant aspects of the individual case, and, in particular, the evidence submitted by that undertaking.[40] This examination must be mirrored in the reasons laid down in the Commission's decision.[41] In particular, the Commission cannot disregard an economic study provided by the dominant undertaking to demonstrate that its conduct is not capable of producing effects, without setting out the reasons why it considers the study to be irrelevant to the assessment of the capability of the conduct in question to produce effects, and without giving the dominant undertaking an opportunity to submit additional evidence to replace it.[42] This thought applies similarly to the specific cases of an undertaking submitting an 'as efficient competitor test' showing that its conduct was not capable to foreclose an equally efficient competitor,[43] and an undertaking submitting a counterfactual analysis challenging the Commission's assessment of the causal link between the conduct at issue and its capability to produce effects.[44]

This distinctly differs from the Union Courts' earlier judgments, such as *Hoffmann-La Roche*, in its implementation of an effects-based approach: the effects of the dominant undertaking's conduct are no longer considered at an abstract level on the basis of the type of conduct in question alone. Rather, the effects that conduct has on competition must be examined in concrete terms in each individual case.[45] Having to show the capability

---

[37] See *Intel I* (n 35) paras 138-139.

[38] Most of these more recent judgments were preliminary rulings concerning national competition authorities or Courts. However, as the aim of this article is to help understanding the evidentiary law implications of the Commission's Draft Guidelines, I will focus here on proceedings before the Commission.

[39] *Servizio Elettrico Nazionale* (n 11) para 51; *Unilever Italia* (n 24) para 54; *Google Shopping* (n 16) para 265; *Intel II* (n 16) para 330.

[40] *Servizio Elettrico Nazionale* (n 11) para 52; *Unilever Italia* (n 24) para 54. It seems that this is occasionally understood in a way that the Commission would have to examine *all* aspects of the individual case. In fact, the case law limits the obligation of the Commission to examine the *relevant* aspects.

[41] *Intel II* (n 16) para 332.

[42] *Unilever Italia* (n 24) para 55.

[43] ibid para 60.

[44] Case T-612/17 *Google and Alphabet v Commission* EU:T:2021:763 para 379; confirmed by *Google Shopping* (n 16) paras 227-230.

[45] Similarly: Fernando Castillo de la Torre, 'Is the Effects-Based Approach Too Cumbersome?' in Adina Claici, Assimakis Komninos, and Denis Waelbroeck (eds), *The Transformation of EU Competition Law* (Wolters

to produce effects in each individual case opens the possibility of 'rebuttal', i.e. the possibility for a dominant undertaking to bring forward arguments and evidence suggesting that in the present case, its conduct lacked the requisite capability. Importantly, this does not lead to a reversal of the burden of proof regarding the capability of the conduct to produce effects.[46] The burden of proof lies and remains with the Commission.[47] In its judgment in *Google Shopping*, the Court of Justice stated this regarding the causal link between the dominant undertaking's conduct and the capability to produce effects in unusually clear language. The General Court held that, regarding this causal link, a dominant undertaking may bring forward a counterfactual analysis in order to challenge the Commission's assessment.[48] The Court of Justice found that in doing so, the General Court did not reverse the burden of proof borne by the Commission.[49] In other words, a dominant undertaking does not have to show that its conduct was not capable of having exclusionary effects. It is sufficient for the dominant undertaking to merely call into question this capability, supported by evidence.[50]

In the first place, it is for the Commission to plausibly show that a conduct is capable of producing exclusionary effects.[51] Importantly, the case law does not, however, presuppose a finding of actual exclusionary effects by the Commission or the Courts,[52] and it stresses the Commission's ability to rely on different analytical templates[53] when showing the capability of conduct to have exclusionary effects.[54] In doing so, the case law stays far behind the Commission's former self-commitment to show consumer harm and foreclosure effects individually in each case.[55]

Such analytical templates may include the specific legal tests the case law created for certain types of conduct.[56] It is not entirely clear, however, whether these tests will be

---

Kluwer 2023) 145, 177, however stressing that the Courts do not provide a clear standard as to the degree of detail of this analysis.

[46] See Schweitzer and de Ridder (n 1) 237; similarly, Castillo de la Torre (n 45) 177-178.

[47] Regulation 1/2003 (n 2) Article 2; *Intel II* (n 16) para 328.

[48] *Google and Alphabet* (n 44) para 379.

[49] *Google Shopping* (n 16) para 228.

[50] The Commission has phrased this as a 'reversal of the evidentiary burden of proof', i.e. the burden to produce arguments and evidence, see European Union, 'The Standard and the Burden of Proof in Competition Law Cases' (OECD Best Practice Roundtable on the standard and burden of proof in competition law cases, 5 December 2024), para 83 <https://www.oecd.org/en/events/2024/12/the-standard-and-burden-of-proof-in-competition-law-cases.html> accessed 1 September 2025. This is opposed to the 'legal burden of proof', i.e. which party bears the risk of losing if a certain requirement is not shown to the full conviction of the Court.

[51] This follows from Article 2 of Regulation 1/2003 (n 2) and has been explicitly stated by the Court of Justice in *Intel II* (n 16) para 328.

[52] *Servizio Elettrico Nazionale* (n 11) para 53: 'The purpose of Article 102 TFEU is to penalise abuse by one or more undertakings of a dominant position within the internal market or in a substantial part of it, irrespective of whether such practice has proved successful'. In the same vein: *Unilever Italia* (n 24) para 41; *Intel II* (n 16) para 176.

[53] This is most probably what the Draft Guidelines refer to when the state that 'the case-law has developed tools which can be broadly described and conceptualised […] as "presumptions"', see Draft Guidelines (n 7) fn 131.

[54] *Unilever Italia* (n 24) para 44; *European Superleague* (n 13) para 130; *Google Shopping* (n 16) para 166.

[55] The German Federal Ministry of Economic Affairs and Climate Action welcomes this 'attempt to move away from the more economic approach in individual cases to an approach with economically informed rules', see 'Contribution to the Commission's consultation on the draft Guidelines on exclusionary abuses of dominance', 2 <https://competition-policy.ec.europa.eu/public-consultations/2024-article-102-guidelines_en> accessed 1 September 2025.

[56] Castillo de la Torre (n 45) 177; Pauer (n 23) 124.

sufficient in and of themselves for the Commission to reach the conclusion that certain conduct is capable of producing effects. Looking at the origin of the Court of Justice's recent case law on the need to analyse effects in the individual case in *Intel*, one could assume that the older analytical templates developed by the Union Courts suffice to find the capability to produce effects in the first place: The Court of Justice refers to the handling of rebate schemes under *Hoffmann-La Roche*, and subsequently only sees reason to 'clarify' this jurisprudence regarding the case where the undertaking concerned submits that its conduct was not in fact capable of restricting competition. Only in that specific case would it be for the Commission to examine more specifically the market and conduct in question, going beyond the *Hoffmann-La Roche* test for exclusive dealing.[57]

In later judgments, however, the Court of Justice is less cautious in its phrasing. In *Unilever Italia*, it found that 'it is for the competition authorities to demonstrate the abusive nature of conduct in the light of all the relevant factual circumstances surrounding the conduct in question', which would include, but apparently not be exhaustive of, the circumstances highlighted in defence by the dominant undertaking.[58] The demonstration of the capability to produce effects 'must, in principle, be based on tangible evidence which establishes, beyond mere hypothesis, that the practice in question is actually capable of producing such effects',[59] and while the Commission may rely on 'guidance from economic sciences', it would also be obligated to contextualize this guidance by considering other factors specific to the circumstances of the case, such as the extent of the conduct on the market, capacity constraints on suppliers of raw materials, or the fact that the dominant undertaking is an inevitable trading partner.[60] This approach seems to be adopted by the Court of Justice in all of its recent jurisprudence on the matter.[61]

3 INTERMEZZO: WATCHING THE 'MORE ECONOMIC' APPROACH DIE

Following up on this case law, the Commission's Draft Guidelines now introduce two concepts of presumptions as the next step in the struggle for the evidentiary law standard to assess an allegedly abusive conduct's effects. To understand their relevance from the Commission's point of view, we have to bear in mind the seismic consequences this struggle has already had in the past years. Not only has the Commission's effort to analyse effects in each individual case itself led to more and more prolonged administrative proceedings, but the mixture between this effort by the Commission on the one hand and the Courts setting up a new framework of evidentiary law on the other hand, both happening at the same time, demanded considerable sacrifices. Namely, these sacrifices from the Commission's point of view were *Intel* and *Qualcomm (Exclusivity payments)*. The prohibition

[57] *Intel I* (n 35) paras 137-139.
[58] *Unilever Italia* (n 24) para 40.
[59] ibid para 42.
[60] ibid para 44.
[61] In *European Superleague*, the Court of Justice held that, even when using an analytical template in assessing an allegedly abusive behaviour, this assessment must be carried out 'in the light of all the relevant factual circumstances' and 'on the basis of specific, tangible points of analysis and evidence' concerning the conduct, the market in question, and the functioning of competition on that market, see *European Superleague* (n 13) para 130. The Court of Justice most recently reiterated this formulation in *Google Shopping* (n 16) para 166; and *Intel II* (n 16) para 179.

decisions in both of these cases[62] were ultimately annulled by the Union Courts, both largely on grounds of the effects analysis being carried out erroneously.

In its second judgment in the *Intel* saga, the General Court, after holding the 'as efficient competitor test' relevant for the assessment of the capability to produce effects where it is in fact carried out,[63] extensively analysed the 'as efficient competitor test' conducted by the Commission and found that it was 'vitiated by errors'.[64] The technical errors the General Court found in the Commission's assessment of the 'as efficient competitor test' mainly related to the use of a misleading value in calculating the contestable share of the market and to an extrapolation of results from a short period of time to the entire period of the alleged infringement.[65] Therefore, given Intel's submission that the rebates were not capable of foreclosing an equally efficient competitor, the Commission was not in a position to hold that the conduct at issue was capable of having anti-competitive effects.[66] The General Court consequently annulled the *Intel* prohibition decision, with the Commission's appeal before the Court of Justice ultimately remaining unsuccessful.[67]

Upon Qualcomm's challenge, the General Court also annulled the Commission decision in *Qualcomm (Exclusivity payments)*, on procedural[68] and substantive grounds. On substantive grounds, the General Court essentially found that in the absence of a competitor even capable of meeting Apple's technical requirements, the exclusivity payments could not incentivize Apple not to switch to a competitor,[69] which has been a core element of the Commission's assessment of effects in that case.[70]

4 THE TWO CONCEPTS OF PRESUMPTIONS

Against this background, the Commission's Draft Guidelines on exclusionary abuses, with their two concepts of presumptions, aim at easing the requirements for the effects analysis in certain cases and in accordance with the judgments issued by the Court of Justice. Based on the much-repeated *Hoffmann-La Roche* formula, the Draft Guidelines base their general approach to the concept of abuse under Article 102 TFEU on two pillars: a deviation of the conduct from competition on the merits and a capability of the conduct to have exclusionary

---

[62] See on these above Section 2.2.
[63] Case T-286/09 RENV *Intel Corporation v Commission* EU:T:2022:19 para 126.
[64] ibid para 482.
[65] In detail, see Miroslava Marinova, 'The EU General Court's 2022 Intel Judgment: Back to Square One of the Intel Saga' (2022) 7(2) European Papers 627, 632-633; Martin Toskov, 'Intel Renvoi: The General Court Sets a Course to Steer the EU Through Troubled Waters' (2023) 7(2) European Competition & Regulatory Law Review 125, 127, each with references to the judgment.
[66] *Intel Renvoi* (n 63) para 526.
[67] See *Intel II* (n 16).
[68] For an overview, see Anton Gerber, 'Qualcomm: Numerous Procedural and Substantive Shortcomings Lead to Spectacular Commission Defeat' (2023) 7(3) European Competition & Regulatory Law Review 183, 185 with references to the judgment.
[69] Case T-235/18 *Qualcomm v Commission (Qualcomm – exclusivity payments)* EU:T:2022:358 para 412. Seemingly approving of this, Dirk Auer and Lazar Radic, 'The Growing Legacy of Intel' (2023) 14(1) Journal of European Competition Law & Practice 15, 17. The judgment's somewhat strange unconditional commitment to the 'as efficient competitor' standard and its apparent misunderstanding of the fact that Article 102 TFEU seeks to prohibit the mere risk of distorted competition that comes with certain conduct have been righteously criticized from various perspectives, see Deutscher (n 35) throughout; Gerber (n 68) 187-188; Pauer (n 23) 118-119; Andreas Heinemann, 'Wettbewerbsrecht: Keine Geldstrafe gegen den Chiphersteller Qualcomm' [2022] Europäische Zeitschrift für Wirtschaftsrecht 648, 662.
[70] See Commission Decision in *Qualcomm (Exclusivity Payments)* (n 31) recitals 412-465.

effects.[71] The presumptions I study in this article concern the second of these pillars, i.e. the capability of the conduct to have exclusionary effects.

In paragraph 60 of the Draft Guidelines, the Commission sets out three different legal scenarios in which the dominant undertaking's conduct is capable of having exclusionary effects. Firstly, the capability to have effects is presumed if one of the specific legal tests developed by the case law for certain conduct due to their typically high potential to produce exclusionary effects is met.[72] Secondly, the capability to have effects is presumed in cases of naked restrictions, i.e. if the dominant undertaking's conduct has no economic sense other than restricting competition.[73] And thirdly, in the absence of one of these two cases, the Commission has to assess the capability of the conduct to have exclusionary effects in the individual case, based on specific, tangible points of analysis and evidence.[74] The two concepts of presumptions each follow their own rationale and rules, that I will study in the following.

4.1 PRESUMPTIONS IN CASES OF SPECIFIC LEGAL TESTS

According to paragraph 60b of the Draft Guidelines, a presumption of the conduct's capability to produce effects applies if one of the specific legal tests is met which the Union Courts have set up for certain types of conduct, namely exclusive supply or purchasing agreements, rebates conditional upon exclusivity, predatory pricing, margin squeeze (in the presence of negative spreads) and certain forms of tying.

The Draft Guidelines make it clear that for these types of conduct the capability to have effects is presumed based on the general recognition of their respective high potential to produce exclusionary effects.[75] In other words, economically informed experience suggests that, if certain more easily observable conditions are met, there is typically some capability to produce exclusionary effects. Given this empirical link between the set of facts and the relevant capability, it is only logical to consider an abbreviated analysis of effects to be sufficient at first.[76] Of course, the assessment of these empirical correlations and the observations of such 'typical' scenarios is an inherently economic task, which shows that the use of presumptions does not render the enforcement of the competition rules economically uninformed. Rather, it merely changes the way in which we translate economic insights into law.

This rationale, based on the 'typicality' of certain types of conduct, immediately brings with it the possibility for an undertaking to argue that the case in question lacks this typicality. Since the presumptions follow from empirical reasoning, there is no point to uphold them in cases which withstand the underlying empirical logic. For example, if an undertaking that allegedly entered into abusive exclusivity agreements asserts, based on tangible evidence, that the conduct in question was not capable of foreclosing an equally efficient competitor, that is, in principle, questioning the underlying rationale. If an equally efficient competitor can

---

[71] Draft Guidelines (n 7) para 45. See on this framework, Schweitzer and de Ridder (n 1) 228-234.
[72] Draft Guidelines (n 7) para 60b. See below Sections 4.1; 5.1.
[73] Draft Guidelines (n 7) para 60c. See below Sections 4.2, 5.2-5.3.
[74] Draft Guidelines (n 7) para 60a. For the facts that may be relevant in this assessment, see Draft Guidelines (n 7) paras 68-75.
[75] ibid para 60b.
[76] See, on all this, conceptually, Schweitzer and de Ridder (n 1) 236.

still compete, the exclusivity agreement might neither deprive the customer of its choice, nor deny competitors access to the relevant market. That does not mean that an abusive capability to have exclusionary effects is ruled out per se, but such capability must, absent typicality of the case in question, be set out and proven in detail.

The mechanism for the 'rebuttal' of this presumption by the dominant undertaking shows that the Commission's concept of presumptions is strongly based on recent case law of the Union Courts on the admissibility of analytical shortcuts and submissions by the dominant undertaking. A dominant undertaking can 'rebut' the presumption by submitting, on the basis of supporting evidence, that its conduct was not capable of having exclusionary effects.[77] As an example of such a submission, the Draft Guidelines cite the case in which a dominant undertaking would show that the circumstances of the case at hand differ substantially from the assumptions underlying the presumption, to the point where any exclusionary effect is purely hypothetical.[78] Additionally, the case law includes cases in which an undertaking submits an 'as efficient competitor test' showing that its conduct was not capable to foreclose an equally efficient competitor,[79] or a counterfactual analysis challenging the Commission's assessment of the causal link between the conduct at issue and its capability to produce effects.[80]

This submission by the dominant undertaking thus is the basis for the Commission's further assessment. The Commission examines the undertaking's submission, or, in other words: '[t]he submissions put forward by the dominant undertaking during the administrative procedure determine the scope of the Commission's examination obligation'.[81] So, while the burden of proof regarding the capability to produce effects is not at all moved away from the Commission,[82] the presumption is narrowing the way for the Commission to prove said capability. To come to the conclusion that the dominant undertaking's conduct is capable of having exclusionary effects, the Commission can either show that the submission by the dominant undertaking is not sufficient to call into question the presumption, or it can provide additional evidence – based on the submission of the dominant undertaking – that shows

---

[77] Draft Guidelines (n 7) para 60b with references to the case law.
[78] ibid para 60b.
[79] *Unilever Italia* (n 24) para 60.
[80] *Google and Alphabet* (n 44) para 379; confirmed by *Google Shopping* (n 16) paras 227-230.
[81] Draft Guidelines (n 7) para 60b. Critically regarding the incentives created for the dominant undertaking to 'flood' (original German: 'überschwemmen') the Commission with submissions, see Carsten König, 'Praktikabilität durch Vermutungen?' [2024] Neue Zeitschrift für Kartellrecht 485, 486.
[82] This mechanism has repeatedly been misinterpreted in the sense that it would – contrary to what the Draft Guidelines, in accordance with the settled case law, state – bestow upon the dominant undertaking the burden of proof regarding the rebuttal. See, for an illustrious example, Akman, Fumagalli, and Motta (n 10) 9. Akman, Fumagalli & Motta have even suggested that the presumptions might *de facto* be irrebuttable (p 9). This suggestion seems quite far off, given the burden of proof lies and remains with the Commission throughout the process, both according to the case law and according to the Draft Guidelines.
The American Bar Association's Antitrust Law and International Law Sections have submitted that this should be made explicit in the final guidelines, see 'Comments of the American Bar Association Antitrust Law Section and International Law Section on the European Commission's Draft Exclusionary Abuse Guidelines', 6 <https://competition-policy.ec.europa.eu/public-consultations/2024-article-102-guidelines_en> accessed 1 September 2025; similarly the Austrian Federal Ministry of Labour and Economy, 'Stellungnahme des Österreichischen Bundesministeriums für Arbeit und Wirtschaft zum Entwurf einer Mitteilung der Europäischen Kommission "Leitlinien für die Anwendung von Artikel 102 des Vertrags über die Arbeitsweise der Europäischen Union auf Fälle von Behinderungsmissbrauch durch marktbeherrschende Unternehmen"', 7-8 <https://competition-policy.ec.europa.eu/public-consultations/2024-article-102-guidelines_en> accessed 1 September 2025.

the capability of the relevant conduct to exert effects. Even in this second case, the presumption continues to carry at least some evidentiary weight.[83]

For exclusive dealing and exclusivity rebates, the Draft Guidelines include a list of specific factors to be assessed in the case of a 'rebuttal' of the presumption: The extent of the dominant position, the share of the market affected by the conduct, the conditions of the exclusivity agreement, such as their duration, and the possible strategy aimed at excluding a competitor.[84] This may be laid down in the part of the Draft Guidelines specifying exclusive dealing, considering that the examples stem from cases regarding exclusivity agreements,[85] yet most of these facts seem of general interest beyond such cases.[86] At least the extent of the dominant position and the possibility of a strategy to exclude competitors have been recognized relevant for other types of conduct, too.[87]

At first glance, the benefit of such a mechanism from the perspective of the Commission and the public interest in an effective enforcement of Article 102 TFEU might seem small.[88] A look at how the mechanism could work out in practice proves this impression wrong: an example from the Commission's decisional practice heretofore can, again, be found in its *Qualcomm (Exclusivity payments)* case.[89] Arguing that its conduct was not capable of producing any exclusionary effect, Qualcomm submitted an 'as efficient competitor test' meaning to show that a competitor equally efficient to Qualcomm could have covered the relevant costs to poach Apple despite the exclusivity payments, had Apple made the choice to switch to them.[90] The Commission concluded Qualcomm's test to be insufficient to call into question the 'presumption' as it was based on 'unrealistic or incorrect assumptions', such as unrealistically low costs an equally efficient competitor had to bear, or the fact that the contestable share of Apple's LTE chipset requirements was in fact smaller than assumed in the test.[91] If we consider only the scope of the Commission's assessment of the 'as efficient competitor test' as measured in pages of the Commission's prohibition decision, we find that

---

[83] Draft Guidelines (n 7) para 60b.
[84] ibid para 83 with references to the case law.
[85] See *Intel I* (n 35) paras 138-139; *Unilever Italia* (n 24) para 48; *Intel II* (n 16) para 331.
[86] However, some cautiousness is appropriate in applying any of said criteria to other types of conduct, given that, for predatory pricing, the General Court has explicitly held the market coverage of the conduct irrelevant for an effects assessment in Case T-671/19 *Qualcomm v Commission (Qualcomm – predation)* EU:T:2024:626 para 522.
[87] See *Google Shopping* (n 16) para 265.
[88] Magali Eben and David Reader, 'Response to European Commission Consultation on Draft Guidelines on the application of Article 102 TFEU to exclusionary abuses of dominance', 7 <https://competition-policy.ec.europa.eu/public-consultations/2024-article-102-guidelines_en> accessed 1 September 2025; Assimakis Komninos, "'J'accuse!" – Four Deadly Sins of the Commission's Draft Guidelines on Exclusionary Abuses' (*Network Law Review*, 30 August 2024) <https://www.networklawreview.org/komninos-guidelines/> accessed 1 September 2025: 'a very weak presumption, whose practical value for public enforcement is minimal'. Similarly: Miroslava Marinova, 'Reply to the European Commission Public Consultation on the Draft Guidelines on the Application of Article 102 TFEU to Exclusionary Abuses', para 4.15 <https://competition-policy.ec.europa.eu/public-consultations/2024-article-102-guidelines_en> accessed 1 September 2025, who suggests that the Commission sets out clear cases in which it will not accept a rebuttal via an 'as efficient competitor test'.
[89] For the facts of the case, see above Section 2.2.
[90] Commission Decision in *Qualcomm (Exclusivity Payments)* (n 31) recital 487. See also, Kadar, 'Article 102 and Exclusivity Rebates in a Post-Intel World' (n 30) 445; Romana Hajnovicova, Ngoc-Lan Lang, and Andrea Usai, 'Exclusivity Agreements and the Role of the As-Efficient-Competitor Test After Intel' (2019) 10(3) Journal of European Competition Law & Practice 141, 147-148.
[91] Commission Decision in *Qualcomm (Exclusivity Payments)* (n 31) recitals 490-503.

in this case, the Commission discusses Qualcomm's submission in merely five pages. In *Intel*, on the other hand, where the Commission carried out the test itself, this takes up 151 pages. It has been estimated that conducting this test alone took the Commission two years.[92] This comparison may be shallow, but it certainly is useful as an exemplary indicator of the complexity of the Commission's assessment. It shows that the Commission's ability to rely on analytical shortcuts initially and only assess an undertaking's submissions instead of fully analysing the capability to produce effects in each case considerably facilitates the proceedings from the Commission's perspective.[93]

4.2 PRESUMPTIONS IN CASES OF NAKED RESTRICTIONS

According to paragraph 60c of the Draft Guidelines, a presumption of the conduct's capability to produce exclusionary effects also applies to naked restrictions, i.e. types of conduct that have no economic interest for the dominant undertaking, other than that of restricting competition. As examples, the Draft Guidelines list payments by a dominant undertaking to customers that are conditional upon the customers postponing or cancelling the launch of products featuring products offered by the dominant undertaking's competitor, agreements obligating distributors to swap a competing product with the dominant undertaking's product under threats to withdraw discounts and the dismantling by the dominant undertaking of infrastructure used by its competitors.

The presumption in cases of naked restrictions differs significantly from the presumption in cases of specific legal tests, originating in the underlying rationale, that is more normative than empirical.[94] The concept of naked restrictions refers to conduct by dominant undertakings that has no economic sense other than excluding competitors, and can therefore be described as inherently improper. A case that has been described as 'perhaps the most blatant abuse that the European Commission has ever considered'[95] is *Baltic Rail*:[96] In the wake of losing a customer to a competitor, the dominant undertaking dismantled a piece of railroad infrastructure, thereby making its competitor's offer impossible.

While there is broad agreement on the fact that this is a case that hits the very core of the concept of an abuse under Article 102 TFEU,[97] the underlying 'no economic sense' rationale does not provide enforcement with an empirical typicality to lead to exclusionary

---

[92] See Wouter Wils, 'The Judgment of the EU General Court in Intel and the So-Called "More Economic Approach" to Abuse of Dominance' (2014) 37(4) World Competition 405, 431.
[93] See also Pauer (n 23) 123-124 with further references.
[94] However, naked restrictions do as well follow a partially empirical rationale, see Schweitzer and de Ridder (n 1) 239. For the fitting example of predatory pricing below AVC, see below Section 5.2.
[95] Pablo Ibáñez Colomo, 'GC Judgment in Case T-814/17, Lithuanian Railways—Part I: object and indispensability' (*Chillin'Competition*, 1 December 2020) <https://chillingcompetition.com/2020/12/01/gc-judgment-in-case-t%E2%80%91814-17-lithuanian-railways-part-i-object-and-indispensability/> accessed 1 September 2025.
[96] *Baltic Rail* (Case AT.39813) Commission Decision of 2 October 2017. See, in more detail, below Section 5.3[b].
[97] See Michele Giannino, 'Lithuanian Railways: The Court of Justice Narrows Down the Scope of Application of the Doctrine of Essential Facilities' (2023) 7(4) European Competition and Regulatory Law Review 260, 263; Massimiliano Kadar, Johannes Holzwarth, and Virgilio Pereira, 'Abuse of Dominance under Article 102 TFEU: a Survey on 2023' (2024) 15 Journal of European Competition Law & Practice 278, 281; Ibáñez Colomo, 'GC Judgment in Case T-814/17' (n 95); Niamh Dunne, 'Dispensing with Indispensability' (2020) 16(1) Journal of Competition Law & Economics 74, 102: 'absurdist proportions'.

effects, as required for the above type of presumptions.[98] Rather, conduct is prohibited because it does not come with the rationale of profit maximization through superior performance, as is an integral part of normal competition.[99] Such behaviour is not worth protecting: In this sort of 'clear cut' abuse cases that lack any pro-competitive and thus socially valuable rationale, the social costs of a falsely positive prohibition decision are drastically reduced. It is suitable in these situations to presume the capability of the conduct to produce exclusionary effects.

This different rationale has implications on the functioning of the presumption, as well, especially concerning the possibility of rebuttal. According to the Draft Guidelines, the dominant undertaking can prove that its conduct was not capable of having exclusionary effects only 'in very exceptional cases',[100] but there apparently remains room for the presumption to be rebutted. The draft is silent on what would be required for such a rebuttal. Given the normative rather than empirical reasoning underlying the presumption, the logic of presumptions in cases of specific legal tests cannot be applied to naked restrictions. If it is not the typical capability to exert effects in certain circumstances that triggers the presumption, there is no point in giving the dominant undertaking the chance to submit that the case in question lacks such typicality.

The dominant undertaking would thus, to rebut the presumption, have to prove that its conduct – even though lacking any pro-competitive rationale – was not in fact capable of producing exclusionary effects. In other words, the presumption in cases of naked restrictions amounts to a full reversal of the burden of proof regarding the conduct's capability to have effects. In not having an authority's possibilities to investigate the relevant facts, especially garnering the immense amount of information required about the market conditions, establishing such a lacking capability to have effects to the full conviction of the Court presents a dominant undertaking with insurmountable challenges.[101] Contrary to the wording of the Draft Guidelines, the presumption in cases of naked restrictions is not rebuttable only 'in very exceptional cases', but it is *de facto* irrebuttable.[102]

That it is irrebuttable does not in itself render such a presumption generally inadmissible. The Court of Justice previously held that it lies within the special responsibility

---

[98] As Gregory J Werden puts it in 'Identifying Exclusionary Conduct Under Section 2: The "No Economic Sense" Test' (2006) 73(2) Antitrust Law Journal 413, 417: 'The test [the "no economic sense test"] does not condemn conduct undertaken because of an unreasonable belief that the conduct would have an exclusionary effect. […] But exclusionary conduct is condemned even if the decision maker's rationale for undertaking the conduct was not profit maximization: Burning down a rival's factory is exclusionary conduct even if the defendant is a pyromaniac and never considers the economic benefits of the conduct'.

[99] The presumption in cases of naked restrictions also shows how the two pillars of the abuse test are intertwined: Where conduct has no economic sense but exclusion, this deviates most thoroughly from normal competition and, in turn, the requirements to show a capability to produce effects are lowered. Although the Draft Guidelines do not make it explicit, their wording is generally open to apply this logic beyond the cases of presumptions as well. If neither 'no economic sense' nor a specific legal test apply, the finding of an abuse ultimately comes down to an interplay between the two pillars.

[100] Draft Guidelines (n 7) para 60c.

[101] See, to that respect, Schweitzer and de Ridder (n 1) 236; John M Taladay, 'The use of presumptions in antitrust enforcement and jurisprudence' (2024) 4 Concurrences 30, paras 59-60.

[102] For a different point of view, see Pablo Ibáñez Colomo, 'On the Article 102 TFEU Guidelines (II): 'naked restrictions' (or 'by object' abuses)' (*Chillin'Competition*, 19 November 2024) <https://chillingcompetition.com/2024/11/19/on-the-article-102-tfeu-guidelines-ii-naked-restrictions-or-by-object-abuses/> accessed 1 September 2025, who sees room for a rebuttal in cases where there are 'no real and concrete possibilities' of entry in the market concerned.

borne by an undertaking in a dominant position not to engage in practices the implementation of which holds no economic interest other than eliminating competitors, and that such practices are inherently at odds with competition on the merits.[103] Under certain circumstances, such a deviation from competition on the merits alone may be sufficient to establish an abuse according to the case law,[104] which most likely refers to a finding of 'no economic sense'.[105] To prevent the finding of an abuse, an undertaking can of course argue that its allegedly 'naked' conduct in fact comes with some pro-competitive rationale in the circumstances of the specific case, i.e. that the 'no economic sense test' triggering the presumption is not met in the first place.[106] Also, an undertaking engaging in naked restrictions can still resort to showing that its conduct is objectively justified.[107] In contrast, the fact that a presumption is irrebuttable is of considerable value to the workability of public enforcement. Where the 'no economic sense test' is fulfilled, the Commission can skip the analysis of effects altogether and reach a prohibition decision faster. However, these considerations call for particular caution in the application of the presumption in cases of naked restrictions and especially for a thorough examination of the underlying 'no economic sense test' in each individual case.[108]

5 THE RELEVANT TESTS TO TRIGGER THE PRESUMPTIONS

To trigger one of the presumptions from the Draft Guidelines, the Commission either has to establish the conditions of the respective legal test the case law has developed for the type of conduct at hand (para 60b) or find that the dominant undertaking's conduct has no economic interest for that undertaking, other than that of restricting competition (para 60c). In the following sections, I will study these different tests in an attempt to highlight certain ambiguities that remain when applying them, starting with the 'specific legal tests' from the past case law and continuing with the 'no economic sense test' and its application to price-based and non-price-based conduct.

5.1 THE SPECIFIC LEGAL TESTS FOR CERTAIN TYPES OF CONDUCT

The presumption in cases of specific legal tests applies to four types of conduct: Exclusive dealing (including exclusivity rebates);[109] predatory pricing above average variable costs

---

[103] *Servizio Elettrico Nazionale* (n 11) para 77. See Draft Guidelines (n 7) para 54.
[104] *Unilever Italia* (n 24) para 57.
[105] This shows, again, the intertwining of the effects analysis and the assessment of a deviation from competition on the merits, see above n 99.
[106] See on the details of the 'no economic sense test' below at Sections 5.2-5.3.
[107] Draft Guidelines (n 7) para 60c. Highlighting the potentially unlimited possibilities for such an objective justification, see Gregory J Werden, 'Comments of Gregory J. Werden on Draft Article 102 Guidelines' (*SSRN*, 5 September 2024), para 56 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4946326> accessed 1 September 2025.
[108] See on the details of that test, below Sections 5.2-5.3. To not provoke an all to cautious application, Giorgio Monti seems sceptical of understanding para 60c as an irrebuttable presumption, see 'Comments on "Guidelines on the application of Article 102 of the Treaty on the Functioning of the European Union to abusive exclusionary conduct by dominant undertakings"', para 33, <https://competition-policy.ec.europa.eu/public-consultations/2024-article-102-guidelines_en> accessed 1 September 2025.
[109] Draft Guidelines (n 7) para 78 with references to *Hoffmann-La Roche* (n 15) para 89; *Intel I* (n 35) para 137. It is also sufficient to show that a different obligation, e.g. a stocking or volume requirement, is de facto

(AVC) or average avoidable costs (AAC), yet below average total costs (ATC) or long-run average incremental costs (LRAIC), that is part of a plan to eliminate or reduce competition;[110] margin squeeze, if the price-cost-test shows that the spread between the upstream and downstream prices is negative;[111] and 'certain forms' of tying.

For tying, the Draft Guidelines remain particularly blurry on where to draw the line to presume the capability to produce effects. In accordance with the case law, the tying and tied products must be two separate products, the undertaking concerned must be dominant in the market for the tying product and it must not give customers a choice to obtain the tying product without the tied product.[112] In addition, to trigger the presumption, it must be possible to conclude that, due to the specific characteristics of the markets and products at hand, the tying has a high potential to produce exclusionary effects, which is the case especially in situations where the inability of competitors to enter or expand their presence in the tied market is likely to directly result from the tying conduct due to the absence of clearly identifiable factors that could offset the exclusionary effects.[113] This is all but a clear standard.[114] Therefore, it can only really be assumed for typical, straightforward cases of tying having an obvious effect of leveraging.

In contrast, the Draft Guidelines state two cases in which the presumption could not in any way apply: when the tied product is available for free and when it is easy to obtain alternatives to the tied product.[115] In these cases, the customers are realistically not deprived

---

playing out to be an exclusivity agreement, see Draft Guidelines (n 7) paras 79 and 81 with references to the case law.

[110] Draft Guidelines (n 7) para 111b with references to the case law, especially Case C-62/86 *AKZO v Commission* EU:C:1991:286 para 72. If the prices charged by the dominant undertaking are below AVC or AAC, the undertaking 'is presumed to pursue no economic objective other than eliminating its competitors', see Draft Guidelines (n 7) para 111a with references to the case law, especially Case C-62/86 *AKZO v Commission* EU:C:1991:286 para 71. Consequently, in the system of the Draft Guidelines, such behaviour is a naked restriction and subject to the second category of presumptions (contrary to what the Draft Guidelines state in para 112), see also Pablo Ibáñez Colomo, 'Draft Guidelines on exclusionary abuses: comments', slide 11 <https://competition-policy.ec.europa.eu/public-consultations/2024-article-102-guidelines_en> accessed 1 September 2025. In more detail, see below Section 5.2.

If the costs are above AVC or AAC, yet below ATC or LRAIC, the low-pricing strategy is not a naked restriction, because it can in fact have a pro-competitive rationale: under these circumstances, an equally efficient competitor could still compete with the dominant undertaking without suffering losses unsustainable in the long run, making it possible for the dominant undertaking's strategy to be desired price competition instead of an abusive exclusionary strategy. See, to that respect, Case C-209/10 *Post Danmark* EU:C:2012:172 para 38. See further on this below Section 5.2. Considering a dominant undertaking's potentially higher financial resources compared to equally efficient competitors, such conduct still comes with a high potential to foreclose these competitors, see Case C-62/86 *AKZO v Commission* EU:C:1991:286 para 72.

[111] Draft Guidelines (n 7) para 122a-b, read in conjunction with paras 124 and 128. If the spread is negative, there is no need to further examine the capability to produce effects in the first place, according to para 128, as then the presumption is triggered. This differentiation in the handling between margin squeeze in the presence of negative spreads and margin squeeze in the presence of positive spreads is firmly grounded in the case law: The Court of Justice held in *TeliaSonera* that if the spread is negative, i.e. the wholesale price for an input service is higher than the retail price for the service to the end user, even equally efficient competitors are probably excluded as they will want to prevent selling at losses; such a probability cannot be detected in a situation where the spread is positive, see Case C-52/09 *TeliaSonera Sverige* EU:C:2011:83 paras 73-74.

[112] Draft Guidelines (n 7) para 89 with references to Case T-604/18 *Google and Alphabet v Commission (Google Android)* EU:T:2022:541 para 284; Case T-201/04 *Microsoft v Commission* EU:T:2007:289 paras 842, 859, 862, 864, 867, 869, 1144-1167.

[113] Draft Guidelines (n 7) para 95 and especially fn 233 with references to Case T-30/89 *Hilti v Commission* EU:T:1991:70; Case T-83/91 *Tetra Pak International v Commission* EU:T:1994:246.

[114] This is also a point of critique for the Austrian Federal Ministry of Labour and Economy (n 82) 8.

[115] Draft Guidelines (n 7) para 95 with references to the case law.

of their choice in the first place, making it necessary to take a closer look at the circumstances of the individual case to assess whether the conduct could nevertheless lead to a leveraging of market power by the dominant undertaking. Factors to include in the examination of the capability of a tying practice to exert effects are whether the dominant undertaking also enjoys dominance on the market for the tied product, the significance of the link between the tying and the tied product (e.g. the complementarity of the products), the presence of barriers to entry in the tied market, the degree of consumer inertia or bias in the tied market,[116] the duration of the conduct[117] and the extent of the tying practice[118] in terms of the share of customers tied. These factors, especially where already known to the Commission, may also be of relevance for triggering the presumption in cases of tying, considering the blurry standard as depicted above. Additionally, in the above cases of 'atypical' tying, given they lack a firm foundation in classical theories of harm, the Commission may, exceptionally, be required to establish actual exclusionary effects, such as the actual marginalisation or exit of competitors in the tied market or an actual increase in the barriers to entry and expansion on that market.[119]

In the same vein, there might be reason to consider a broader range of aspects of the individual case when applying the other specific legal tests, too. Not only would it be a better solution policy-wise by ensuring that the public enforcement is based on a dynamic and economically sound and up-to-date reading of the case law.[120] Even more, it could ultimately prove risky for the Commission to rely on legal tests, some of which are quite superficial and derive from decades old case law, considering the newer developments in the Union Courts' jurisprudence.[121] To date, it is not entirely clear if such presumptions based only on the specific legal tests for certain types of conduct will stand up in Court. As pointed out above,[122] in newer judgments, the Court of Justice holds that, even when the Commission relies on analytical templates, the assessment of effects has to be 'made in the light of all the relevant factual circumstances […] on the basis of specific, tangible points of evidence'.[123]

The question arises as to whether the specific legal tests as described above meet the requirements of case law on analytical templates.[124] This is probably true for predatory pricing and margin squeeze: Triggering the presumption in these cases presupposes conducting a price-cost-test anyway, therefore being thoroughly grounded in the peculiarities of the individual case. The situation is rather different regarding exclusive dealing, in which the presumption is triggered on grounds of a fairly superficial and abstract analytical template.

---

116 For all these, see Draft Guidelines (n 7) para 94 with references to the case law.
117 ibid para 95 with references to the case law.
118 ibid para 70d.
119 ibid para 95. See, to this respect, also Schweitzer and de Ridder (n 1) 238.
120 Similarly, Pablo Ibáñez Colomo, 'The (Second) Modernisation of Article 102 TFEU' (2023) 14(8) Journal of European Competition Law & Practice 608, 619-620 who speaks of 'proxies' and 'bright lines'. Ultimately in the same vein: Berkeley Research Group, 'Response to the European Commission's public consultation on the Draft Guidelines on the application of Article 102 TFEU to exclusionary conduct', para 38 <https://competition-policy.ec.europa.eu/public-consultations/2024-article-102-guidelines_en> accessed 1 September 2025.
121 Harsher: Komninos, '"J'accuse!"' (n 88): 'at variance with existing case law'; Komninos, 'The European Commission's Draft Guidelines on Exclusionary Abuses' (n 10): 'arbitrary and form-based'.
122 Section 2.3.
123 *European Superleague* (n 13) para 130; *Google Shopping* (n 16) para 166; *Intel II* (n 16) para 179. Put differently, but essentially saying the same: *Unilever Italia* (n 24) paras 42, 44.
124 Seemingly favourable of the sufficiency, Castillo de la Torre (n 45) 177.

All it presupposes is the finding of an exclusivity requirement or incentivizing scheme.[125] To avoid failing before the Courts, the Commission should consider widening its first assessment in these cases to (at least some of) the factors it holds relevant for the examination of effects in cases of exclusive dealing. These include the extent of the dominant position, the share of the market affected by the conduct, the conditions of the exclusivity agreement, such as their duration, and the possible strategy aimed at excluding a competitor.[126]

5.2 PRICE-BASED NAKED RESTRICTIONS: PREDATORY PRICING BELOW AVC

The presumption in cases of naked restrictions in turn presupposes a finding that the dominant undertaking's conduct has no economic interest for that undertaking, other than that of restricting competition. Under this test, any pro-competitive rationale suffices to eliminate the presumption from the game.[127] Accordingly, the Commission lists only three examples of possible naked restrictions, and has in fact been even more cautious in its previous decisional practice, with the *Intel* case being the only example of the Commission actually relying on the concept of naked restrictions to find an abuse. A manifest differentiation must be made in this regard between price-based conduct and other types of conduct by dominant undertakings.

This differentiation helps operationalizing the 'no economic sense test', as conduct by a dominant undertaking concerning the pricing of its products and services will typically come with the possibility of a pro-competitive rationale to support it and thus fail the test. As prices are the most standard parameter of competition, the freedom of an undertaking to unilaterally set its prices according to its own costs and business strategy generally remains untouched by competition law.[128] In principle, this also applies to below-cost pricing: some of the reasons for which an undertaking may opt for such a strategy are not particularly probable in cases of dominant undertakings,[129] but it may nevertheless be rational for dominant undertakings under certain circumstances, such as where the pricing strategy is built upon the complementarity of products.[130] Even without complementarity in a technical sense, it may still be rational for the dominant undertaking to sell certain products below

---

[125] See Draft Guidelines (n 7) para 78.

[126] See for this, ibid para 83 with references to the case law, as well as the respective sections in para 70. The type of exclusive dealing in question hence can influence the exact scope of the effects analysis: Is it for example 'only' a stocking requirement incentivizing the customer to purchase exclusively from the dominant undertaking, the Commission might want to take a closer look at the conduct and market in question than it would in case of a flat-out formal obligation to exclusively purchase.

[127] See Eric B Rasmusen, J Mark Ramseyer, and John S Wiley Jr, 'Naked Exclusion' (1991) 81(5) The American Economic Review 1137: 'conduct unabashedly meant to exclude rivals, for which no one offers any efficiency justification'. See also Schweitzer and de Ridder (n 1) 239-240 with a discussion of whether the newer case law on restrictions by object under Article 101 TFEU might be significant in modifying this condition.

[128] The same idea calls for caution in applying the concept of exploitative abuses to prices, see Ernst-Joachim Mestmäcker and Heike Schweitzer, *Europäisches Wettbewerbsrecht* (3rd edn, C.H. Beck 2014) 439 with further references.

[129] For example gaining consumers' goodwill is typically not going to be a priority for an already dominant undertaking, see Chiara Fumagalli, Massimo Motta, and Claudio Calcagno, *Exclusionary Practices: The Economics of Monopolisation and Abuse of Dominance* (Cambridge University Press 2018) 84.

[130] ibid 85.

costs and cross-finance this with other sales.[131] Another possible explanation for prices below cost includes 'fire sales' of goods that are considered excess or obsolete by the seller.[132]

Price-based conduct may only come with no economic sense for the dominant undertaking except restricting competition under the conditions of the first step of the Union Courts' predatory pricing test. In that regard, the Court of Justice has held in *AKZO* that prices that come below AVC have no economic sense other than eliminating competitors.[133] The above explanations for pricing below costs do not materialise when the prices are even below AVC. In these cases, the conduct in question amounts to a naked restriction.[134]

Given the fact that a price-cost-test needs to be carried out to establish predatory pricing below AVC in the first place, classifying such conduct as a naked restriction may come with limited practical consequences, however. Furthermore, where a price-cost-test indicates prices below AVC, such conduct also tends to be not replicable by an equally efficient competitor and therefore come with a high probability of exclusionary effects. This case blurs the boundaries between the two concepts of presumptions studied in this paper. Yet, even if a dominant undertaking would come forward with arguments and evidence suggesting that in the specific case at hand, its conduct was not capable of producing exclusionary effects (and thereby rebut the probability of effects), this alone is not sufficient to rule out the finding of 'no economic sense' that comes with the observation of prices below AVC.

5.3 OTHER TYPES OF CONDUCT: FROM INTEL TO BALTIC RAIL AND BEYOND

In the realm of non-price-based conduct, the 'no economic sense test' might potentially play a bigger role. For conduct that is not price-based, there cannot be an initial assumption of pro-competitiveness as it is not *prima facie* concerning a parameter of competition. Accordingly, the examples the Draft Guidelines list from the Commission's past decisional practice revolve around non-price-based conduct: payments by a dominant undertaking to customers that are conditional upon the customers postponing or cancelling the launch of products featuring products offered by the dominant undertaking's competitor (modelled after *Intel*), agreements obligating distributors to swap a competing product with the dominant undertaking's under threats to withdraw discounts (modelled after *Irish Sugar*), and the dismantling by the dominant undertaking of infrastructure used by its competitors (modelled after *Baltic Rail*). This list is, of course, not conclusive, as the relevant test stays the

---

[131] See, to that respect, the examples at Franz Böhm, *Wettbewerb und Monopolkampf* (Carl Heymanns 1933) 298-300.

[132] In *Qualcomm (predation)*, the dominant undertaking submitted that instead of eliminating a competitor, such 'fire sales' were the explanation for its low pricing strategy, see *Qualcomm (predation)* (n 86) para 585.

[133] *AKZO* (n 110) para 71. For the relation between AVC and AAC, see Draft Guidelines (n 7) para 115.

[134] Pablo Ibáñez Colomo, 'Persistent myths in competition law (V): "there is no such thing as an abuse by object (or by effect) under Article 102 TFEU"' (*Chillin'Competition*, 10 January 2020) <https://chillingcompetition.com/2020/01/10/persistent-myths-in-competition-law-v-there-is-no-such-thing-as-an-abuse-by-object-or-by-effect-under-article-102-tfeu/> accessed 1 September 2025; Pablo Ibáñez Colomo, 'Agree or disagree, abuses "by object" are a thing unless the case law changes' (*Chillin'Competition*, 12 January 2022) <https://chillingcompetition.com/2022/01/12/agree-or-disagree-abuses-by-object-are-a-thing-unless-the-case-law-changes/> accessed 1 September 2025. See to that respect *Qualcomm (predation)* (n 86) para 521: 'there being no need for the Commission to undertake any analysis other than such a comparison of the prices charged by the dominant undertaking and of some of its costs'.

'no economic sense test'. In identifying naked restrictions and in delineating further cases, the examples might prove helpful, however. I will therefore continue by examining the cases underlying the examples and tentatively deducing more general thoughts that might stand behind them.

5.3[a] Intel and Irish Sugar

The relevant part of the *Intel* case was about Intel directing payments towards three OEMs – HP, Acer and Lenovo – for cancelling or delaying the launch of certain products that included its competitor AMD's x86 CPUs.[135] The Commission concluded that it could not 'discern any economic justification in the conducts'.[136] Intel argued that, given AMD's performance, the Commission had not adequately proven the effects of the relevant conduct.[137] The Commission found that not only was it not required to show a foreclosure effect,[138] but it considered its assessment of the actual effect of the conduct in form of cancellation and delays of AMD-based products, depriving customers of a choice they would have otherwise had, sufficient.[139]

The idea might arise that Intel's payments to the OEMs, as it was facing severe competition from AMD, amount to mere 'price competition' and hence are generally excluded from the category of naked restrictions if the overall pricing of Intel's x86 CPUs – taking into account the relevant payments – would not come below AVC. However, this fails to take into account that Intel did in fact not just lower its CPU prices to compete with AMD, but in requiring the OEMs to cancel or delay the commercialization of AMD-based products, it provoked agreements which in and of themselves may defy any pro-competitive rationale. There might be an initial argument to liken Intel's conduct to an 'exclusivity agreement light', as the OEMs did not fully pledge to only purchase from Intel, but rather, agreed just to halt a certain competitor's product. Compared to a situation of exclusivity, however, the classic pro-competitive benefits do not materialize in such conduct; exclusivity agreements may have a pro-competitive rationale because they guarantee long-lasting sales and supply, rendering long-term planning easier feasible and creating economies of scale, and they can contribute to solving hold-up problems.[140] Such explanations do not apply to Intel's conduct at hand, however: the agreement to merely delay the commercialization of a competitor's product does not foster any of the usual reasons brought forward to justify exclusivity agreements. Against this background, a pro-competitive business rationale for such conduct seems, indeed, hard to find. Therefore, the Commission was right to assume that Intel's payments conditional upon its customers postponing or cancelling the launch of products featuring products offered by its competitor

---

135 Commission Decision in *Intel* (n 28) recitals 1641 et seq. See also *Intel* (Case AT.37990) Commission Decision of 22 September 2023, in which the Commission re-imposed the fines for naked restrictions, after the original *Intel* decision's suspension by *Intel Renvoi* (n 63) leaving the Commission's reasoning in the uncontested section about naked restrictions untouched.

136 Commission Decision in *Intel* (n 28) recital 1680.

137 ibid recital 1668.

138 ibid recital 1669 with reference to Case T-219/99 *British Airways v Commission* EU:T:2003:343 para 298.

139 Commission Decision in *Intel* (n 28) recital 1670.

140 See Mestmäcker and Schweitzer (n 128) 455; Jonathan M Jacobson and Scott A Sher, '"No Economic Sense" Makes No Sense for Exclusive Dealing' (2006) 73 Antitrust Law Journal 779, 788-790 with further references; Fiona M Scott Morton, 'Contracts that Reference Rivals' (2013) 27(3) Antitrust 72, 75.

amounted to naked restrictions.[141]

In its arguing in the *Intel* case, the Commission heavily relied on its own decision[142] and the judgment of the General Court[143] in *Irish Sugar*. One of the relevant conducts in this case was the so-called 'product swap'. After the commercialization of a competitor's product – the 1 kilogram packet of 'Eurolux' sugar – the dominant undertaking Irish Sugar agreed with one wholesaler and one retailer to exchange its own sugar with Eurolux sugar.[144] Although Irish Sugar claimed that it was due to the insufficient demand for the poorly marketed Eurolux sugar, the Commission found that the goal of the product swap was to prevent Eurolux from gaining any market presence in Ireland[145] and that it resulted in a consolidation of Irish Sugar's almost monopoly position as supplier of sugar in Ireland.[146] Perhaps even more so than in *Intel*, this conduct appears void of any pro-competitive rationale.

5.3[b] Baltic Rail

The case underlying the Commission's decision in *Baltic Rail*[147] epitomizes the concept of an abuse of dominance under Article 102 TFEU to an extent where the facts of the case would be somewhat imaginative or unbelievable, were they not real. The dominant Lithuanian railroad undertaking LG was in the wake of losing a customer in the railway freight business, the producer of refined oil OL, to the Latvian railroad undertaking LDZ.[148] OL transported oil from its refinery in Lithuania to or through Latvia, having contracted LG for the short route from the refinery to the Latvian border, and LDZ for the rest of the way in Latvia. OL wanted to switch from LG to LDZ for the route from its refinery to the Latvian border, and also change is seaborne export business from Lithuanian ports to Latvian ports, transporting the cargo with LDZ. In reaction to these plans, LG dismantled a 19 kilometres piece of railroad that was exclusively used to transport OL's products to Latvia.[149]

Even though the Commission carried out an extensive analysis of effects in this case,[150] it is fairly straightforward to assume that LG's conduct in fact did not have any economic interest but to exclude LDZ and, thus, restrict competition. Therefore, a detailed analysis of effects was obsolete.[151] Before the Courts, LG argued that its dismantling of the tracks amounted to a refusal of access to an essential facility, therefore triggering the application of the *Bronner* criteria to answer the question as to whether LG was obligated under

[141] Similarly, Pauer (n 23) 120-121, speaking of 'prima facie anticompetitiveness'.
[142] *Irish Sugar plc* (Cases IV/34.621, 35.059/F-3) Commission Decision 97/624/EC [1997] OJ L258/1.
[143] Case T-228/97 *Irish Sugar v Commission* EU:T:1999:246.
[144] Commission Decision in *Irish Sugar* (n 142) recital 124.
[145] ibid recital 125.
[146] ibid recital 126. The Commission's reasoning was upheld in *Irish Sugar* (n 143) paras 228-234.
[147] Commission Decision in *Baltic Rail* (n 96); substantially confirmed by Case T-814/17 *Lietuvos geležinkeliai v Commission* EU:T:2020:545 and Case C-42/21 P *Lietuvos geležinkeliai v Commission* EU:C:2023:12.
[148] On the facts of the case, see Commission Decision in *Baltic Rail* (n 96) recitals 16-113.
[149] The Commission nicely illustrates this with a series of somewhat comical photographs of the railroad track in question abruptly ending in the middle of nowhere, see Commission Decision in *Baltic Rail* (n 96) p 25.
[150] See Commission Decision in *Baltic Rail* (n 96) recitals 202-324. In detail, the Commission found that LDZ exerted considerable competitive pressure upon LG prior to the dismantling of the track (recitals 205-284), LDZ was not able to continue exerting competitive pressure after said dismantling (recitals 285-316) and that led to LDZ's foreclosure from the relevant market (recitals 317-324).
[151] Giannino (n 97) 263; Kadar, Holzwarth, and Pereira (n 97) 281.

Article 102 TFEU to grant LDZ access to the respective track.[152] The Court of Justice dismissed the application of the *Bronner* criteria, highlighting the differences between a denial of access and LG's conduct at hand: By destroying the railroad, LG sacrificed an asset, as the track became unusable not only by its competitors, but also by the dominant undertaking itself.[153] As the Court of Justice understands LG's conduct as entailing a sacrifice borne by the dominant undertaking, it likens this conduct to predatory pricing and thereby seems to acknowledge that this conduct is not plausibly explainable except by an exclusionary objective.[154]

5.3[c] Further applying the 'no economic sense test'

Seemingly casuistic at first, this logic of a 'sacrifice' borne by the dominant undertaking may give a first indication on how to apply the 'no economic sense test' beyond the examples given in the Draft Guidelines. Where a practice is not even profitable for the dominant undertaking in the short-run, a closer look must be taken as to whether such conduct comes with any pro-competitive rationale.

Yet more common ground in the three examples from the Draft Guidelines may be found in the reference of the dominant undertaking's conduct to a specific competitor,[155] detached from its own performance. Intel's conduct targeted AMD, Irish Sugar's conduct targeted the Eurolux sugar, and LG's conduct targeted LDZ – three competitors that put the respective dominant undertakings under serious competitive pressure, and three cases in which the dominant undertaking is setting up measures specifically targeting the challenger. Generalizing this idea, if the dominant undertaking is referencing a specific competitor in its conduct, or targeting this competitor with its conduct, this may be another indication that the behaviour – absent the specific competitor's exclusion – does not bear any economic sense. This might include extreme *Baltic Rail*-style cases where a dominant undertaking is destroying a competitor's facilities,[156] or even removing a competitor's products and merchandise from retail stores,[157] but it also might include more subtle *Intel*-style cases of payments or discounts conditional upon some conduct engaging with a competitor.

Since the 'no economic sense test' follows a similar logic as the most clear-cut cases of

[152] See Case C-42/21 P *Lietuvos geležinkeliai v Commission* EU:C:2023:12 paras 62-63.
[153] ibid paras 83-84.
[154] Giannino (n 97) 263. See also Opinion of AG Rantos in Case C-42/21 P *Lietuvos geležinkeliai v Commission* EU:C:2022:537 paras 78-79: 'that behaviour was motivated only by the willingness to harm competitors'.
[155] Generally on the concept of 'contracts that reference rivals', see Scott Morton (n 140). Scott Morton defines this category as 'contracts containing material terms that are contingent not only on the prices or quantities transacted between the parties to the contract, but also on the prices, quantities, or other terms of the relationship between one of the parties and product market rivals of the other'. Examples given by Scott Morton include exclusive dealing, most-favored-nation provisions, meet-or-release provisions and loyalty rebates. See also, Fumagalli and Motta (n 10) 94, deeming 'practices that reference rivals' presumptively unlawful.
[156] See Werden, 'Identifying Exclusionary Conduct Under Section 2: The "No Economic Sense" Test' (n 98) 417.
[157] See for example *Conwood Co., L.P. v U.S. Tobacco Co.*, 290 F 3d 768 (2002). On this, see David T Scheffman and Richard S Higgins, 'Twenty Years of Raising Rivals' Costs: History, Assessment, and Future' (2003) 12 George Mason Law Review 371, 385-387.

a deviation from competition on the merits,[158] the facts which the Commission holds relevant for an assessment of said deviation may as well play a role.[159] Especially the cases in which an undertaking provides misleading information to administrative or judicial authorities, or misuses regulatory procedures,[160] and whether the undertaking violates rules in other areas of law thereby affecting relevant parameters of competition[161] may provide important clues on the rationale pursued by that undertaking and hence, whether the conduct can be explained as pro-competitive.

Such aspects may be the first step for the Commission in the assessment of the 'no economic sense test', but there still is need to properly assess each individual case of unilateral conduct, contextualized by the undertakings and markets in question as well as the rationale of said conduct, against the standard of the 'no economic sense test'. When taking the aspects from above into account, there are essentially two scenarios in which the limitations of such considerations become apparent.

In the first scenario, the aspects laid out above apply to certain conduct that is well-known to come with a pro-competitive explanation. In these cases, the Commission cannot conclude 'no economic sense', and the finding of a naked restriction is ruled out in general. Rather, the Commission would have to resort to the presumption in cases of specific legal tests or a showing of the capability to produce exclusionary effects in the individual case. For example, exclusive dealing is one of the most straightforward cases of a contract referencing a rival. Yet, it may of course be pro-competitive.[162]

In the second scenario, absent a specific type of conduct that is well-known to have pro-competitive benefits, the dominant undertaking can also bring forward arguments, supported by evidence, that its conduct in the individual case can be explained as pro-competitive. It would then be for the Commission, and ultimately for the Union Courts, to decide whether the dominant undertaking actually pursued a pro-competitive rationale with its allegedly abusive conduct. This examination may ultimately coincide with the assessment of a possible efficiency defence.

6 CONCLUDING THOUGHTS

A historical perspective on the struggle for the evidentiary law standard regarding the question whether a dominant undertaking's conduct is capable to produce exclusionary effects shows that an effects-based approach to abuse of dominance is not a static concept. Rather, different varieties of such an effects-based approach are conceivable in principle and observable in practice. Certainly, some of these varieties do not keep pace with the passing of time and the progress of economic insight; others fail to meet the practical needs of

[158] See above n 99. In the system of the Draft Guidelines, this is also illustrated by the fact that a finding of 'no economic sense' also leads to an automatic finding of a deviation from competition on the merits, see Draft Guidelines (n 7) para 54.
[159] Monti (n 108) para 31.
[160] Draft Guidelines (n 7) para 55b with reference to Case C-457/10 P *AstraZeneca v Commission* EU:C:2012:770 paras 98 and 134. Also: Monti (n 108) para 31: 'the two abuses in *Astra Zeneca* are not only inherently suspect when carried out by domco but, in the relevant legal and economic context, reveal in themselves a harm to competition'.
[161] Draft Guidelines (n 7) para 55c with reference to Case C-252/21 *Meta Platforms and Others (General terms of use of a social network)* EU:C:2023:537 paras 47 and 51.
[162] See Scott Morton (n 140) 73-75. The same goes for the other examples given in n 155.

an enforcement authority. The presumptions I have studied in this paper, and the Union Courts' recent judgments they are based on, manifest one such variety that is both aware of the deficiencies of overly simplistic legal tests in light of modern possibilities to assess potential effects in individual cases, and driven by a realistic understanding of the value a functioning system of enforcing the competition rules has.

The Commission's Draft Guidelines contain two distinct concepts of presumptions that can facilitate the Commission's assessment of an allegedly abusive conduct's capability to produce exclusionary effects. The presumptions in cases of specific legal tests follow the empirical rationale that certain types of conduct bear a particularly high potential to produce exclusionary effects. In these cases, a superficial assessment of the conduct's capability to produce such effects will suffice in the first place. For a rebuttal of these presumptions, the dominant undertaking must merely call into question the typicality of the case at hand, supported by evidence: the burden of proof remains with the Commission at all times. In contrast, with the presumption in cases of naked restrictions, i.e. conduct that has no economic interest for the dominant undertaking except that of restricting competition, the burden of proof shifts to the dominant undertaking, *de facto* rendering the presumption irrebuttable. This is due to its normative rather than empirical rationale, expressed in the underlying 'no economic sense test'.

While both of these concepts are in principle construed in accordance with the Union Courts' case law on the evidentiary law of Article 102 TFEU, and both of them come with significant advantages from an enforcer's perspective, it is still uncertain to what extent the presumptions will meet the expectations that are set for them. For the presumptions in cases of specific legal tests, it is not entirely clear if the Commission's approach to simply rely on the specific legal tests developed in the past case law is reasonable from a policy perspective, or even stands up to the Court's requirement of an assessment of all the relevant aspects of the individual case.

For the presumption in cases of naked restrictions, facts to take into account while specifying the underlying 'no economic sense test' may include whether the dominant undertaking bestows upon itself a 'sacrifice', whether the dominant undertaking's conduct references a specific competitor, as well as clear-cut cases of a deviation from competition on the merits. However, the Commission cannot find 'no economic sense' – even when given one of these facts – if there is reason to believe that the conduct in question comes with some pro-competitive rationale, e.g. if such pro-competitiveness is well-known for the type of conduct or proven by the undertaking in the individual case. How narrow or broad this test can be understood to be, which additional facts may be relevant in conducting it and how helpful the presumption can prove to be amidst its necessarily narrow construction is a matter of future development.

In all this, not only do the two concepts of presumptions not defy an effects-based approach to abuse of dominance, but rather they offer a reading of the case law that has the potential to positively shape the enforcement of Article 102 TFEU in the years to come. Until the next variety of an effects-based approach to abuse of dominance comes along.

LIST OF REFERENCES

Akman P, 'A Critical Inquiry into "Abuse" in EU Competition Law' (2024) 44(2) Oxford Journal of Legal Studies 405
DOI: https://doi.org/10.1093/ojls/gqae008

Akman P, Fumagalli C, and Motta M, 'The European Commission's draft guidelines on exclusionary abuses: a law and economics critique and recommendations' [2025] Journal of European Competition Law & Practice <https://doi.org/10.1093/jeclap/lpaf020> accessed 1 September 2025
DOI: https://doi.org/10.1093/jeclap/lpaf020

Auer D and Radic L, 'The Growing Legacy of Intel' (2023) 14(1) Journal of European Competition Law & Practice 15
DOI: https://doi.org/10.1093/jeclap/lpac055

Barbera A, Fajardo Acosta N, and Klein T, 'The Role of the AEC Principle and Test in a Dynamic and Workable Effects-Based Approach to Abuse of Dominance' (2023) 14(8) Journal of European Competition Law & Practice 582
DOI: https://doi.org/10.1093/jeclap/lpad057

Böhm F, *Wettbewerb und Monopolkampf* (Carl Heymanns 1933)
DOI: https://doi.org/10.5771/9783845227214

Castillo de la Torre F, 'Is the Effects-Based Approach Too Cumbersome?' in Claici A, Komninos A, and Waelbroeck D (eds), *The Transformation of EU Competition Law* (Wolters Kluwer 2023)

Deutscher E, 'Causation and counterfactual analysis in abuse of dominance cases' (2023) 19(3) European Competition Journal 481
DOI: https://doi.org/10.1080/17441056.2023.2219440

Di Giovanni Bezzi R, 'A Tale of Two Cities: Effects Analysis in Article 102 TFEU Between Competition Process and Market Outcome' (2023) 14(2) Journal of European Competition Law & Practice 83
DOI: https://doi.org/10.1093/jeclap/lpad004

Dunne N, 'Dispensing with Indispensability' (2020) 16(1) Journal of Competition Law & Economics 74
DOI: https://doi.org/10.1093/joclec/nhaa004

Fumagalli C and Motta M, 'Economic Principles for the Enforcement of Abuse of Dominance Provisions' (2024) 20(1-2) Journal of Competition Law & Economics 85
DOI: https://doi.org/10.1093/joclec/nhae003

Fumagalli C, Motta M, and Calcagno C, *Exclusionary Practices: The Economics of Monopolisation and Abuse of Dominance* (CUP 2018)
DOI: https://doi.org/10.1017/9781139084130

Gerber A, 'Qualcomm: Numerous Procedural and Substantive Shortcomings Lead to Spectacular Commission Defeat' (2023) 7(3) European Competition & Regulatory Law Review 183
DOI: https://doi.org/10.21552/core/2023/3/10

Giannino M, 'Lithuanian Railways: The Court of Justice Narrows Down the Scope of Application of the Doctrine of Essential Facilities' (2023) 7(4) European Competition and Regulatory Law Review 260
DOI: https://doi.org/10.21552/core/2023/4/13

Hajnovicova R, Lang NL, and Usai A, 'Exclusivity Agreements and the Role of the As-Efficient-Competitor Test After Intel' (2019) 10(3) Journal of European Competition Law & Practice 141
DOI: https://doi.org/10.1093/jeclap/lpz019

Heinemann A, 'Wettbewerbsrecht: Keine Geldstrafe gegen den Chiphersteller Qualcomm' [2022] Europäische Zeitschrift für Wirtschaftsrecht 648

Ibáñez Colomo P, 'The (Second) Modernisation of Article 102 TFEU' (2023) 14(8) Journal of European Competition Law & Practice 608
DOI: https://doi.org/10.1093/jeclap/lpad064

Jacobson JM and Sher SA, '"No Economic Sense" Makes No Sense for Exclusive Dealing' (2006) 73(3) Antitrust Law Journal 779

Kadar M, 'Article 102 and Exclusivity Rebates in a Post-Intel World' (2019) 10(7) Journal of European Competition Law & Practice 439
DOI: https://doi.org/10.1093/jeclap/lpz041

— —, 'Evaluating 20 Years of Regulation 1/2003: Are EU Antitrust Procedures "Fit for the Digital Age"?' (2024) 85(3) Antitrust Law Journal 577

Kadar M, Holzwarth J, and Pereira V, 'Abuse of Dominance under Article 102 TFEU: a Survey on 2023' (2024) 15(4) Journal of European Competition Law & Practice 278
DOI: https://doi.org/10.1093/jeclap/lpae032

König C, 'Praktikabilität durch Vermutungen?' [2024] Neue Zeitschrift für Kartellrecht 485

Lauer R, 'The Intel saga: what went wrong with the Commission's AEC test (in the General Court's view)?' (2024) 20(1) European Competition Journal 45
DOI: https://doi.org/10.1080/17441056.2023.2242698

Marinova M, 'The EU General Court's 2022 Intel Judgment: Back to Square One of the Intel Saga' (2022) 7(2) European Papers 627
DOI: https://doi.org/10.15166/2499-8249/590

McCallum L et al, 'A dynamic and workable effects-based approach to abuse of dominance' (Competition Policy Brief No 1/2023) <https://op.europa.eu/en/publication-detail/-/publication/ef8f0a39-cf77-11ed-a05c-01aa75ed71a1/language-en> accessed 1 September 2025

Mestmäcker EJ and Schweitzer H, *Europäisches Wettbewerbsrecht* (C.H. Beck 2014)

Mestmäcker EJ, *Das marktbeherrschende Unternehmen im Recht der Wettbewerbsbeschränkungen* (Mohr Siebeck 1959)

Nazzini R, *The Foundations of European Union Competition Law* (Oxford University Press 2011)
DOI: https://doi.org/10.1093/law-ocl/9780199226153.001.0001

Neven DJ, 'The As-Efficient Competitor Test and Principle' (2023) 14(8) Journal of European Competition Law & Practice 565
DOI: https://doi.org/10.1093/jeclap/lpad063

Pauer NI, 'From Intel & Qualcomm to the new Art. 102 TFEU-Guidelines' (2024) 22(2) Zeitschrift für Wettbewerbsrecht 115
DOI: doi.org/10.15375/zwer-2024-0205

Rasmusen EB, Ramseyer JM, and Wiley JS Jr, 'Naked Exclusion' (1991) 81(5) The American Economic Review 1137

Rohner T, *Art. 102 AEUV und die Rolle der Ökonomie* (Nomos 2023)
DOI: https://doi.org/10.5771/9783748941071

Scheffman DT and Higgins RS, 'Twenty Years of Raising Rivals' Costs: History, Assessment, and Future' (2003) 12(2) George Mason Law Review 371

Schweitzer H and de Ridder S, 'How to Fix a Failing Art. 102 TFEU' (2024) 15(4) Journal of European Competition Law & Practice 222
DOI: https://doi.org/10.1093/jeclap/lpae033

Scott Morton FM, 'Contracts that Reference Rivals' (2013) 27(3) Antitrust 72

Taladay JM, 'The use of presumptions in antitrust enforcement and jurisprudence' (2024) 4 Concurrences 30

Toskov M, 'Intel Renvoi: The General Court Sets a Course to Steer the EU Through Troubled Waters' (2023) 7(2) European Competition & Regulatory Law Review 125
DOI: https://doi.org/10.21552/core/2023/2/9

Werden GJ, 'Identifying Exclusionary Conduct Under Section 2: The "No Economic Sense" Test' (2006) 73(2) Antitrust Law Journal 413

— —, 'Comments of Gregory J. Werden on Draft Article 102 Guidelines' (*SSRN*, 5 September 2024) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4946326> accessed 1 September 2025
DOI: https://doi.org/10.2139/ssrn.4946326

Wils W, 'The Judgment of the EU General Court in Intel and the So-Called "More Economic Approach" to Abuse of Dominance' (2014) 37(4) World Competition 405
DOI: https://doi.org/10.54648/woco2014042

FREE MOVEMENT, MUTUAL RECOGNITION AND HOMOGENEITY: THE CASE OF HEALTH WORKERS IN THE EU AND EEA

MARÍA CAMILA SALAZAR LARSEN[1*]

The principle of mutual recognition, grounded in mutual trust, anchors the free movement of professionals within the European Union (EU), assuming that qualifications awarded in one Member State (MS) will be accepted across the region. However, despite the EEA agreement and the principle of homogeneity extending these rules to EFTA States, practical challenges, particularly in sectors like healthcare, reveal inconsistencies in how mutual recognition is applied in the labour market. While the EU and EEA frameworks aim to create a barrier-free single labour market, delays in the incorporation of EU legislation, bureaucratic obstacles, national differences in qualification requirements due to education systems being primarily regulated at a national level, and language barriers continue to hinder effective mobility and the proper application of the principle of homogeneity in the framework of the EEA Agreement. This article highlights key EFTA Court rulings that clarify Member States' obligations under Directive 2005/36/EC and the EEA Agreement, especially regarding timely legislative implementation, proportionality of language requirements, and the need for accessible recognition mechanisms. Ultimately, while public health grounds may justify certain limitations, the EFTA Court has reinforced legal principles aimed at safeguarding the freedom of movement for health professionals[2] across the EU and EEA. Strengthening inter-institutional cooperation at the EU level, between employment and education ministries, is essential to align training programs with labour market needs and to harmonize qualification standards in regulated professions, ensuring effective mutual recognition and the free movement of professionals in line with the principle of homogeneity. This discussion is particularly timely due to the recent own initiative cases opened by the EFTA Surveillance Authority against Norway and the enactment of Directive EU 2024/782, which will enter in force in 2026.[3]

1 INTRODUCTION

The European Parliament stated in 2017 that the European Union (EU) single market 'constitutes the largest barrier-free, common economic space in the industrialized world, encompassing over half a billion citizens in an economy with a gross domestic product

[1*] Faculty of Law, University of Bergen, Norway. LL.M. in EU and EEA Law. Scholarship recipient of the EEA Social Security Law Research Project in collaboration with the University of Bergen, University of Oslo, and University of Tromsø.

[2] When referring to Health Workers, this article addresses in general the professions of nurses, midwives, doctors, dentists, and pharmacists. While this article generally considers the aforementioned professions, it should be noted that the selected case law of the EFTA Court refers specifically to the professions of doctors, dentists, and psychologists.

[3] I would like to express my sincere gratitude to Professors Christian Franklin, Ingrid Margrethe Halvorsen Barlund, and Melanie Regine Hack for their invaluable guidance and for imparting their extensive knowledge of institutional and internal market law within the EU/EEA. Their continuous encouragement and support have been instrumental in fostering my intellectual curiosity and creativity.

(GDP) of some €13 trillion'.[4] Furthermore, the creation of the single market has increased employment by 2.8 million and added 2.2% to the GDP of the EU.[5] A single labour market in the EU has given people the chance to work and travel around the EU as freely as within a single country.[6] In fact, 17 million EU citizens live or work in an EU country other than their own.[7] In addition, it is important to highlight that, in 1992, the creation of the European Economic Area (EEA) agreement granted access to the internal market to the EFTA states (Norway, Iceland, and Liechtenstein). However, despite the apparent success of the internal market and the opportunities it offers, not all professionals benefit equally from it, as significant barriers still hinder the full exercise of free movement rights, particularly for health professionals. In fact, the EU is a unique environment for the mobility of health professionals that showcases benefits, but also constraints.[8]

To understand the challenges health professionals face in exercising their free movement rights, it is first necessary to examine the legal architecture underpinning the EU and EEA internal market framework. To begin with, the EU is a sui generis international organization, subject to and of international law. The TEU determines that its aim is to 'promote economic and social progress for their peoples […] within the context of the accomplishment of the internal market'.[9] To be able to accomplish a single market, Member States (MS) have had to transfer part of their regulatory autonomy to the EU.[10] On the other hand, the EEA Agreement allows Norway, Iceland and Liechtenstein to participate in the internal market and enjoy the four freedoms established in the EU. As has been mentioned by Fredriksen and Franklin (2015) 'the EU is by far the most important trading partner of the EFTA States and a significant number of their companies and citizens exercise their rights to free movement to and within the EU'.[11] To be able to join the internal market, the EFTA states must include relevant EU legislation in their legal systems to guarantee homogeneity between the EU and the EEA and an effective participation in the internal market for all actors.[12]

As was mentioned before, the legal framework of the EU's internal market is built on

---

[4] European Parliament, 'EU Single Market: Boosting Growth and Jobs in the EU' (Briefing, European Added Value in Action, 2017) <https://www.europarl.europa.eu/RegData/etudes/BRIE/2017/611009/EPRS_BRI(2017)611009_EN.pdf> accessed 1 September 2025.

[5] 'EU Single Market: Boosting Growth and Jobs in the EU' (n 2).

[6] European Council, '30th anniversary of the EU single market' (last reviewed 28 July 2025) <https://www.consilium.europa.eu/en/infographics/30-years-of-the-eu-single-market/> accessed 1 September 2025.

[7] European Council, 'EU Single Market' (5 February 2025) <https://www.consilium.europa.eu/en/policies/deeper-single-market/> accessed 1 September 2025.

[8] James Buchan et al (eds), 'Health Professional Mobility in a Changing Europe: New Dynamics, Mobile Individuals and Diverse Responses' (European Observatory on Health Systems and Policies, WHO 2014) <https://iris.who.int/handle/10665/326372> accessed 1 September 2025.

[9] Consolidated Version of the Treaty on the Functioning of the European Union [2016] OJ C202/195 (TFEU), preamble.

[10] The legal basis for the transfer of sovereignty can be found in Articles 1, 4 and 5 of the TEU and Articles 2 and 3 of the TFEU, as well as in case law such as the Case C-6/64 *Costa v E.N.E.L.* EU:C:1964:66.

[11] HH Fredriksen and CNK Franklin, 'EEA Law and the EU Internal Market: A Growing Tension' (2015) 52 Common Market Law Review 629 https://doi.org/10.54648/cola2015049

[12] As has been mentioned by the EEA authorities 'the number of legal acts incorporated into the EEA Agreement varies from year to year. Typically, the number falls somewhere between 500 and 600 legal acts'. For more information: <https://www.efta.int/about-efta/frequently-asked-questions> accessed 1 September 2025.

four fundamental freedoms: the free movement of goods, capital, persons, and services. Within the freedoms of persons and services, the mutual recognition of professional qualifications plays a central role, as it enables individuals to exercise their acquired skills, which can be done on a permanent basis under the free movement of workers and establishment, or on a temporary basis under the freedom to provide services.[13]

Throughout this article, the analysis will focus on the exercise of the free movement of persons, in particular the free movement of workers and the freedom of establishment for the self-employed. This has been the most common context in which individuals have encountered barriers to exercising their acquired skills across different MS, as reflected in the case law of the EFTA Court, which will be examined below. It should be noted, however, that within the framework of the free movement of services, individuals engaged in liberal professions or undertakings may also face obstacles regarding the recognition and exercise of their professional qualifications across MS. Nevertheless, due to the temporary nature of service provision, this has been a less contested area since to the author's knowledge, no relevant EFTA Court case law exists in this regard. By contrast, the free movement of persons, whether as workers or through self-employment, aims at deeper integration and adaptation to the host Member State. It is therefore in this context that more disputes have arisen, which explains the focus of this article.

The free movement of persons, including the free movement of workers and establishment, is one of the four freedoms recognized in the EU and EEA internal order.[14] This includes the right for workers and the self-employed to move and reside in other MS, rights for family members to join them, equal treatment with nationals and the recognition of their skills to exercise regulated professions.[15] The primary legal basis for the free movement of workers and the self-employed in the EU is directly guaranteed by the Treaty,[16] and can be found in Articles 3(3),[17] 45,[18] 48,[19] 49,[20] 50[21] and 53[22] of the TFEU.

---

[13] The freedom of establishment is analysed under Article 49 TFEU, and not under the scope of Article 56 TFEU, due to the fact that this article focuses on the exercise of professional qualifications on a permanent and not a temporary basis.

[14] The primary legal basis for the free movement of workers can be found on Articles 45-49 of the TFEU. As said by Horspool, Humphreys and Wells-Greco, Article 45 lays down the principles and Article 46 provides detail for implementation – see Margot Horspool, Matthew Humphreys, and Michael Wells-Greco, *European Union Law* (10th edn, Oxford University Press 2018).

[15] Monika Makay and Victor Manuel Martinez Garzon, 'Free Movement of Workers: Fact Sheets on the European Union: European Parliament' (April 2025) <https://www.europarl.europa.eu/factsheets/en/sheet/41/free-movement-of-workers> accessed 1 September 2025.

[16] Manuel Kellerbauer, Marcus Klamert, and Jonathan Tomkin (eds), *The EU Treaties and the Charter of Fundamental Rights: A Commentary* (Oxford University Press 2019).

[17] It establishes the creation of an internal market that aims for full employment and combat exclusion and discrimination.

[18] Establishes the freedom of movement of workers and the abolition of discrimination based on nationality.

[19] Establishes the competence of the European Parliament and Council to adopt ordinary legislative measures in the field of social security to guarantee the free movement of workers across Member States.

[20] Establishes the right to establishment which includes the possibility of conducting activities as self-employed or managing an undertaking. In this article the reference to Article 49 TFEU is conducted, and not to Article 56 TFEU, because this article focuses on the exercise of professional qualifications on a permanent and not temporary basis.

[21] Establishes the duties of the Parliament and the Council in regards to regulating the freedom of establishment.

[22] Establishes that the Parliament and the Council must enact directives for the mutual recognition of diplomas and coordination to recognize qualifications between Member States.

The mentioned articles have been interpreted by the CJEU and developed by secondary legislation.[23] In addition, the guarantees granted in these articles have also been included in the EEA Agreement.[24] One of the most relevant secondary legislation instruments is Directive 2005/36/EC, which establishes a system for the recognition of professional qualifications.[25]

Professional qualifications and certificates awarded in one Member State should be accepted in good faith throughout the EU, according to the principle of mutual recognition which is grounded in the concept of mutual trust between MS.[26] This principle is not only central to the functioning of the internal market but also constitutes a key pillar of the free movement of persons including the free movement of workers and establishment, within the EU and the EEA.

Closely linked to mutual recognition is the principle of homogeneity, which ensures that EFTA States (Norway, Iceland, and Liechtenstein) apply internal market rules in a manner consistent with the EU. For that reason, the principle of mutual recognition must be applied under the scope of the principle of homogeneity, understood as one of the building blocks of the EEA Agreement. In theory, this extends the mutual trust underlying mutual recognition to these countries. Nevertheless, even after 30 years of the EEA Agreement, the application of these principles is not always seamless in practice, particularly in regulated sectors such as healthcare, where discrepancies in recognition of professional qualifications have emerged.

While the EU and EEA legal frameworks establish robust principles supporting free movement and mutual recognition, their effectiveness is heavily shaped by national education systems and the qualification standards set therein. It is fundamental to highlight that MS have retained sovereignty over their national training systems. As set out in Article 165 of the TFEU, the EU may support and supplement national actions in the field of education, but it lacks the competence to harmonize educational systems. Consequently, there is considerable diversity in educational traditions across the EU.

It is important to recognize that education is inherently political, deeply intertwined with national identity and cultural values. Nevertheless, the absence of a centralized or harmonized qualifications framework has tangible consequences for employment opportunities and social mobility within the EU and the EEA, given the close interrelation between education and labour market access. While the European Qualifications Framework (EQF) exists to facilitate comparison of qualifications, it functions primarily as a translation tool rather than a mechanism that ensures substantive alignment of professional standards. As such, it provides limited support to individuals seeking to practise regulated professions in another MS.

This article argues that health professionals who seek to exercise their rights of free

---

[23] Horspool, Humphreys, and Wells-Greco (n 11).

[24] The mentioned legal basis can be found in Articles 28, 29, 30 and 32 of the EEA Agreement.

[25] Directive 2005/36/EC of the European Parliament and of the Council of 7 September 2005 on the recognition of professional qualifications [2005] OJ L 255/22. Directive 2005/36/EC replaced Directive 92/51 and Directive 1999/42. In addition, Directive 2005/36/EC has been amended by various directives that will be showcased further in this paper.

[26] Horspool, Humphreys, and Wells-Greco (n 11) mention that Directive 2005/36/EC was based on two principles: i) mutual trust between Member States and ii) mutual recognition, understood as 'the assumption that certificates awarded in a member state should be accepted in good faith' across the Union.

movement between the EU and the EEA find a set of barriers to effectively migrate as workers from one country to another in detriment to the principle of homogeneity that binds both pillars. The following sections will showcase how the legislative process of the EEA Agreement, bureaucratic processes, additional requirements based on national standards, and language barriers affect the free movement of health professionals and hinder the effective application of the principle of mutual recognition in the single labour market. It will also highlight how the EFTA Court has analysed these issues to present solutions and guarantee and adequate functioning of the EEA Agreement.

2 BARRIERS

The barriers that health professionals encounter in exercising their rights to free movement arise from various sources: some are legal, while others are social, economic, cultural or related to transparency and access to information.[27] This article examines these barriers primarily from an EEA legal perspective, focusing on how delays in the incorporation of relevant EU legislation, lengthy administrative procedures, language requirements and specific host state conditions can hinder the effective exercise of free movement rights. It is important to emphasise, however, that these legal challenges often intersect with broader issues that extend beyond the legal domain.[28]

To begin with, and as stipulated by the EEA Agreement, for an EU legal act to be applicable in the EFTA States, the EEA Joint Committee (JCD) must adopt a decision to incorporate the act into the EEA Agreement.[29] The EEA authorities have specified that the goal is to incorporate these acts as closely as possible to their EU entry-into-force date, ensuring consistent application of rules across the entire EEA.[30]

In the following table some of the most relevant directives and regulations for the recognition of qualifications of health professionals in the EU (incorporated in the EEA Agreement) are listed.

Directive / Regulation	**Summary**	**Incorporated in EEA Agreement**	**Time for Incorporation in EEA Agreement (years)**
Directive	Established the general system for recognition of qualifications for healthcare and related professions. No longer in force since 2007.	2003	2[32]

[27] Buchan et al (n 6).
[28] ibid.
[29] The legal basis for this statement is found in Part VII Chapter 2 of the EEA Agreement.
[30] EFTA Surveillance Authority, 'How EU law becomes EEA Law' <https://www.efta.int/eealaw> accessed 1 September 2025.
[32] European Free Trade Association (EFTA), 'Factsheet – 32001L0019' < https://www.efta.int/eea-lex/32001l0019> accessed 1 September 2025.

Directive / Regulation	Summary	Incorporated in EEA Agreement	Time for Incorporation in EEA Agreement (years)
2001/19/EC[31]			
Directive 2005/36/EC[33]	Created a system for recognition of professional qualifications.	2009	4[34]
Directive 2013/55/EU[35]	Amends Directive 2005/36/EC on recognition of professional qualifications.	2019	6[36]
Directive 2011/24/EU[37]	Established patient rights in cross-border healthcare, with reference to cooperation per Directive 2005/36/EC. Although this Directive does not specifically regulate the recognition of professional qualifications within the region, it remains a relevant instrument as it underscores the importance of cooperation among MS and the need to avoid unnecessary restrictions in the recognition of qualifications, in line with the provisions of Directive 2005/36/EC.[38]	2015	4[39]
Directive	Recognized qualifications of healthcare workers in the context of public	2017	3[41]

[31] Directive 2001/19/EC of the European Parliament and of the Council of 14 May 2001 amending Council Directives 89/48/EEC and 92/51/EEC on the general system for the recognition of professional qualifications and Council Directives 77/452/EEC, 77/453/EEC, 78/686/EEC, 78/687/EEC, 78/1026/EEC, 78/1027/EEC, 80/154/EEC, 80/155/EEC, 85/384/EEC, 85/432/EEC, 85/433/EEC and 93/16/EEC concerning the professions of nurse responsible for general care, dental practitioner, veterinary surgeon, midwife, architect, pharmacist and doctor [2001] OJ L206/1.
[33] Directive 2005/36/EC (n 22).
[34] European Free Trade Association (EFTA), 'Factsheet – 32005L0036' <https://www.efta.int/eea-lex/32005l0036> accessed 1 September 2025.
[35] Directive 2013/55/EU of the European Parliament and of the Council of 20 November 2013 amending Directive 2005/36/EC on the recognition of professional qualifications and Regulation (EU) No 1024/2012 on administrative cooperation through the Internal Market Information System ('the IMI Regulation') [2013] OJ L354/132.
[36] European Free Trade Association (EFTA), 'Factsheet – 32013L0055' <https://www.efta.int/eea-lex/32013l0055> accessed 1 September 2025.
[37] Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare [2011] OJ L88/45.
[38] The aforementioned can be found in the preamble recital 50, Article 2, Article 3(f), and Article 4(5).
[39] European Free Trade Association (EFTA), 'Factsheet – 32011L0024' <https://www.efta.int/eea-lex/32011L0024> accessed 1 September 2025.
[41] European Free Trade Association (EFTA), 'Factsheet – 32014L0024' <https://www.efta.int/eea-lex/32014l0024> accessed 1 September 2025.

Directive / Regulation	Summary	Incorporated in EEA Agreement	Time for Incorporation in EEA Agreement (years)
2014/24/EU[40]	procurement.		
Regulation (EU) 2016/589[42]	Aimed at labour market integration, promoting EURES network for job vacancy and skill matching.	2021	5[43]

It is important to note that Directive (EU) 2024/782 was recently adopted by a Joint Committee Decision (JCD), which also confirmed its entry into force date for the EEA pillar. This new directive amends Directive 2005/36/EC in regards to the minimum training requirements for the professions of nurse responsible for general care, dental practitioner and pharmacist.[44] The aforementioned directive will enter in force in March, 2026.

In the table presented above, it is possible to observe that legal instruments, which are specifically related to the recognition of qualifications of health workers, and that being EEA relevant should be part of the agreement to guarantee an effective movement of workers, have experienced significant delays in incorporation into the EEA legal framework. One can see that duration oscillates between 2 and 6 years. The delay in incorporation creates an important challenge for the free movement of health workers between the EU and the EFTA states, mostly because individuals in the EEA internal order are not able to access justice and enforcement until the norms have been integrated.

It is fundamental for EU relevant legislation to be incorporated in a timely manner to the EEA agreement for a correct functioning and effective participation of EU and EEA workers in the internal market. As has been mentioned by Fredriksen and Franklin (2015) 'timely and correct implementation of the EEA obligations becomes crucial for the proper functioning of the EEA agreement'.

As a consequence, health professionals who seek to exercise their profession in the EFTA states must not only wait for the incorporation of new EU legislation in the internal legal order, but also need to face long administrative processes. The bureaucratic processes differ from member state to member state[45] and can hinder access to recognition in regard to (i) the timeframe to get authorization[46] and (ii) accessibility to the required

[40] Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC [2014] OJ L94/65.
[42] Regulation (EU) 2016/589 of the European Parliament and of the Council of 13 April 2016 on a European network of employment services (EURES), workers' access to mobility services and the further integration of labour markets, and amending Regulations (EU) No 492/2011 and (EU) No 1296/2013 [2016] OJ L107/1.
[43] European Free Trade Association (EFTA), 'Factsheet – 32016R0589' <https://www.efta.int/eea-lex/32016r0589> accessed 1 September 2025.
[44] European Free Trade Association (EFTA), 'Factsheet – 32024L0782' <https://www.efta.int/eea-lex/32024l0782> accessed 1 September 2025.
[45] Edward C Page, 'The European Union and the Bureaucratic Mode of Production' in Anand Menon and Vincent Wright (eds), *From the Nation State to Europe: Essays in Honour of Jack Hayward* (Oxford University Press 2001).
[46] In the case of Norway, estimated waiting time to get approval is between 6 and 8 months. For more information: <https://hkdir.no/en/foreign-education/education-from-outside-of-norway/recognition-of-

information. For instance, the ESA has previously requested Norway to fully comply with the EEA Agreement by reducing its bureaucracy and inaccessibility to online portals such as PSC which assist the recognition of professional qualifications.[47]

A third barrier that health professionals face towards free movement corresponds to the different requirements that must be fulfilled in each member state for each profession on their qualifications framework and the differences on educational programmes. As has been mentioned by Barnard (2022), 'host state rules on the use of professional titles can prove to be a serious impediment for professionals wishing to work in another MS […] given the major differences between the legal systems of the MS'.[48] Even if qualification frameworks in the EU and the EEA should match the European Qualification Framework, each MS can for example provide or require additional certificates at the end of the education programme.[49] At the same time, differences in education programmes can make it difficult to access the spectrums of each profession.

To conclude, it is relevant to highlight that Art 45(3) TFEU determines that it is possible to limit free movement of workers on the grounds of public health, which is replicated in article 28(3) of the EEA agreement. It should be noted that the CJEU has recognised an additional ground for derogation based on overriding reasons of general interest, as established in Case C-351/90.[50] For that reason, the development of the caselaw of the CJEU should be examined alongside the public health derogation. This prerogative has since been incorporated into Directive 2005/36/EC, as reflected in recital 11 of its preamble. Likewise, Article 53 of the Directive 2005/36/EC determines that 'persons benefiting from the recognition of professional qualifications shall have a knowledge of languages necessary for practicing the profession in the host Member State'. As a consequence, there are valid derogations in place that affect the movement of health professionals through different MS with the purpose of protecting public health. Although it is understood as proportional that health professionals should be able to communicate in the local language to guarantee patient safety and a good functioning of the health system in the state of practice, a language requirement creates a practical barrier for those health professionals who want to migrate as workers to a new country. A further discussion of the language requirement will be conducted when presenting the case law of the EFTA Court.

3 APPROACH OF THE EFTA COURT

The practical barriers outlined above have given rise to a series of legal disputes, prompting the EFTA Court to clarify the obligations of EFTA States regarding the implementation and application of mutual recognition rules. In Case E-10/10, the EFTA Court evaluated a case brought by the EFTA Surveillance Authority (ESA) on the failure by Norway to fulfil its

foreign-higher-education-bachelor-master-and-phd/after-you-have-applied-higher-education> accessed 1 September 2025.

47 EFTA Surveillance Authority, 'ESA Asks Norway to Reduce Bureaucracy and Provide Clearer Information for Service Providers' (*EFTA Surveillance Authority*, 5 July 2023) <https://www.eftasurv.int/newsroom/updates/esa-asks-norway-reduce-bureaucracy-and-provide-clearer-information-service> accessed 1 September 2025.

48 Catherine Barnard, *The Substantive Law of the EU: The Four Freedoms* (7th edn, Oxford University Press 2022).

49 Europass, 'National Qualifications Frameworks (Nqfs)' <https://europass.europa.eu/en/europass-digital-tools/european-qualifications-framework/national-qualifications-frameworks> accessed 1 September 2025.

50 Case C-351/90 *Commission v Luxembourg* EU:C:1992:266.

obligations for the incorporation and implementation of Directive 2005/36/EC.[51]

In 2007, the EEA Joint Committee added Directive 2005/36/EC on professional qualifications to the EEA Agreement. It required EFTA States to implement it by 1 July 2009. Norway partially implemented the Directive but notified ESA that amendments to several national regulations were still needed. ESA issued formal notices in late 2009 and early 2010 requesting Norway's compliance, and Norway subsequently informed ESA of gradual progress on the required amendments, with the last updates expected by October 2010. By July 2010, Norway confirmed the implementation of related measures but continued to work on final amendments. The chamber found that Norway did not adopt those measures before the expiry of the time-limit given.

In this ruling it was determined that 'Article 3 EEA imposes upon the Contracting Parties the general obligation to take all appropriate measures, whether general or particular, to ensure fulfilment of the obligations arising out of the EEA Agreement'. On this particular occasion the Court found that Norway did not fulfil its obligations under Article 63 of Directive 2005/36/EC and Article 7 of the EEA Agreement. This was because it did not enact the required measures within the established time frame to implement the Act listed at point 1 of Annex VII to the EEA Agreement, specifically Directive 2005/36/EC on the recognition of professional qualifications, as amended by Regulation (EC) No 1430/2007.

Afterwards, the Case E-1/11 concerned the interpretation of Directive 2005/36/EC under EEA law. In particular, it analyses the recognition of qualifications under EU law in parallel to EFTA states requirements.[52]

In this case an EU trained medical doctor with a psychiatry specialization, applied for a license to practice her profession in Norway but faced challenges with language skills, theoretical knowledge and assessment during her training. The Norwegian Registration Authority rejected her application for full authorisation in August 2009, citing insufficient aptitude for independent practice, though offering her a one-year subordinate medical doctor license. The decision was appealed, and brought before the Norwegian Appeal Board, which requested an Advisory Opinion from the EFTA Court in January 2011.

When analysing the facts of the case, the EFTA Court referred to the case law of the CJEU. In particular, the EFTA Court mentioned the precedent stated in Case C-110/01 (*Tennah-Durez*) and determined that

> an EEA State is not permitted to make the recognition of professional qualifications of doctors meeting the criteria of the Directive subject to any further conditions. The system of automatic recognition would be jeopardized if it were open to EEA States at their discretion to question the merits of a decision taken by the competent

[51] Case E-10/10 *EFTA Surveillance Authority v The Kingdom of Norway* [2010] EFTA Ct. Rep. 312. The legal questions brought up in this case corresponds to identifying if Norway failed to meet its obligations under the EEA Agreement and Directive 2005/36/EC by not implementing the Directive fully within the set time limit.

[52] Case E-1/11 *Norwegian Appeal Board for Health Personnel – appeal from A* [2011] EFTA Ct. Rep. 484. The legal question that concerns the study in this case corresponds to analysing whether EEA law authorizes an EEA state to deny an authorisation to practice as a medical doctor or to grant limited authorisation to an applicant with insufficient professional qualifications, if that person fulfils the requirements provided for in the directive. Likewise, the Court studies if authorisation to practice a health profession can be made subject to further requirements regarding the pursuit of the profession as a doctor, such as knowledge of language.

authority of another EEA State to award the formal evidence of qualification.[53]

The Court also referred to Article 53 of Directive 2005/36/EC, which states that 'persons benefiting from the recognition of professional qualifications shall have a knowledge of languages necessary for the practice of the profession in the host State'. It determined that a doctor's ability to communicate with patients, administrative authorities, and professional bodies constitutes a general public interest and therefore it is justified to require knowledge of the local language to grant authorization.

The Court specified that the assessment of linguistic knowledge is left to individual interpretation of the EEA states. Nevertheless, language requirements should not go far beyond what is necessary to attain the objective of the profession or posting. If an assessment required linguistic abilities that are not part of a normal doctor's work, it would risk being discriminatory or disproportionate.[54] Furthermore, it mentions that EEA state authorities should give the opportunity to acquire missing language skills.

In conclusion, the EEA States are allowed to deny a migrant doctor's authorisation to practice based on personal aptitude issues when the requirements are objectively justified, proportionate to protecting public health and would apply equally to a national doctor, allowing for denial of authorisation if such grounds are present at the time of the evaluation.

At this point, it is important to analyse the existence of the requirement of knowledge of the local language. The case law[55] and doctrine[56] have determined that when assessing a measure it is fundamental to analyse suitability, necessity and proportionality sensu stricto to identify if a restriction is justified.[57]

To begin with, to fulfil the suitability requirement, measures should be adequate 'for securing the attainment of the objective which they pursue and they must not go beyond what is necessary in order to attain it'.[58] Therefore, a requirement to be able to communicate in the local language is suitable for the objective of health professionals and patients being able to appropriately communicate and safeguard patients. In regards to necessity, it has been established that the measure can be justified on public health grounds, which seems appropriate in this scenario because health professionals should be able to understand and be understood by their patients to avoid miscommunications on treatments that could hinder patients' well-being.

Additionally, the measure does not appear to be discriminatory on grounds of nationality, because health professionals that migrate to another state to exercise their profession can access employment on the same grounds as long as they learn and can communicate in the local language.

As has been determined by the case law, 'proportionality sensu stricto entails an assessment of the disadvantages caused by a given measure, and of whether those disadvantages are proportionate to the aims pursued'.[59] As a consequence, the requirement

[53]Case E-1/11 *Norwegian Appeal Board for Health Personnel – appeal from A* [2011] EFTA Ct. Rep. 484. point 66.
[54] Opinion of AG Jacobs in Case C-238/98 *Hocsman* EU:C:1999:426 point 57.
[55] CJEU – Case C-128/22 *NORDIC INFO* EU:C:2023:951; EFTA Court – Case E-19/15 *EFTA Surveillance Authority v the Principality of Liechtenstein* [2016] EFTA Ct. Rep. 437.
[56] Barnard (n 45).
[57] Opinion of AG Emiliou in Case C-128/22 *NORDIC INFO* EU:C:2023:645.
[58] Case C-55/94 *Reinhard Gebhard v Consiglio dell'Ordine degli Avvocati e Procuratori di Milano* EU:C:1995:411.
[59] Opinion of AG Emiliou in *NORDIC INFO* (n 51).

of having sufficient knowledge seems adequate insofar as the objective pursued is that citizens can access a health system that provides them with clear guidelines and seeks to guarantee patient safety. The analysis done by the EFTA Court in Case E-1/11 demonstrates that health professionals are not obliged to have proficiency of the local language for elements that are outside of the normal requirements of the profession, so it is then understood that the requirement is suitable for the objective pursued, and does not exceed what is essential to attain that objective of patient safety.

In Case E-3/20, the EFTA Court studied the case of an EEA national who trained as a dental practitioner in an EU state and who later sought recognition of her qualifications in her EEA home country. In this case, the EEA national received an education as a dental practitioner in Denmark without acquiring a certificate to practice independently in said country.[60]

The EFTA Court concluded that: (i) to benefit from automatic recognition under Article 21(1) of Directive 2005/36/EC, an applicant must hold all certificates required by their home State for the profession listed in Annex V of the Directive; (ii) if an applicant does not meet the automatic recognition criteria, Articles 28 and 31 EEA require the host State to conduct an individual assessment of the applicant's qualifications and training; (iii) this assessment involves comparing the applicant's credentials and experience with the host State's requirements, and if gaps are found, the host State must specify any additional training needed; and (iv) the chamber established that the fact that an applicant does not have full access to the profession in the home State cannot be decisive for the assessment of whether the applicant may be given access to the same profession in the host State.

To end with, Case E-4/20 studied the recognition of professional qualifications of psychologists who had trained in an EU country and subsequently sought to establish themselves in the EEA. In particular, a group of Norwegian citizens obtained a master's degree in psychology from Hungary which did not permit clinical practice. Initially, these individuals were granted licenses. However, the Norwegian authorities changed their policy and revoked them, since the programme did not correspond to the requirements established in Norway. As a consequence, both full and partial authorizations were denied.[61]

The EFTA Court concluded that, to determine if a profession can be considered equivalent in both home and host state, a case-by-case assessment must be completed. The factors that influence if both professions can be deemed the same correspond to aligned core activities, even if there are minor differences.

---

[60] Case E-3/20 *The Norwegian Government v Anniken Jenny Lindberg* [2020] OJ C275/2. The Court formulated three legal questions. In the first place, the Court seeks to analyze the scope of Article 21(1) of Directive 2005/36/EC. In particular to define if evidence of formal qualifications needs to be accompanied by formal certificates. In the second place, the Court seeks to determine whether the host State is under an obligation to examine an application for recognition of qualifications under the scope of the free movement of persons established in the EEA agreement (Articles 28 and 31) when an individual lacks evidence of training according to Article 10 and Article 21 of Directive 2005/36/EC. In the third place, the EFTA Court seeks to provide guidance on the consequences of the applicant not being fully qualified and therefore not having full access to the profession in the home State.

[61] Case E-4/20 Tor-Arne Martinez Haugland and others v The Norwegian Government [2020] OJ C308/21. For our case of study, the relevant legal question in this case corresponds to determining the rules for assessing the equivalence of professions across states for the purposes of Directive 2005/36/EC. As well as if applicants who do not fulfil the requirements of the Directives, can rely on Articles 28 and 31 of the EEA Agreement to pursue a regulated profession in the host state.

On this occasion the court reiterated the rule determined in Case E-3/20 and established that applicants who do not meet recognition requirements under Directive 2005/36/EC can still pursue a regulated profession in the host State by drawing upon Articles 28 and 31 EEA. In these cases, the host State must review all relevant qualifications and professional experience against its own standards and, if there are gaps, specify the additional training needed to meet local requirements.

Building on the legal standards articulated by the EFTA Court, recent enforcement actions by ESA further illustrate the continued gaps in implementation, particularly in the recognition of specific health professions. In particular, ESA has opened an own initiative case (91996) due to the non-availability of aptitude tests as a compensation measure for the profession of nutritionist in Norway.[62] The problem in this case arises from the fact that Norway does not offer a possibility to choose from an aptitude test or an adaptation period, as granted in EEA law.[63] On the contrary, it only offers an adaptation period within limited institutions. Specifically, the ESA states that Norway has failed to fulfil its obligation arising from Directive 2005/36/EC (adapted to the EEA Agreement by Protocol 1) because of the administrative practice of not providing aptitude tests as a compensation measure for health professionals and not providing effective possibilities to access the adaptation period. In September 2024, the Norwegian government was given a period of 2 months to submit its observations.[64]

As a consequence, it is possible to observe that the EFTA Court has had to evaluate the application of the principle of mutual recognition in various occasions and has determined important rules of precedential value:

1) Under Article 7 of the EEA Agreement, EEA states have the obligation to adopt relevant EU legislation into the internal legal order within the timeframe established to avoid a failure to fulfil their obligations and a breach of the agreement. This point is fundamental because the legislative process should not be a reason to hinder full enforcement of the EEA agreement;
2) For the recognition of qualifications of health professionals, as a general rule, States should not ask for further requirements than those established in Directive 2005/36/EC. However, the EFTA Court determined that authorisation to practice a health profession can be made subject to further requirements such as knowledge of the national language. It clarifies that the requirements must be objectively justified, proportionate to protecting public health and would apply equally to a national doctor;
3) In accordance with Article 53 of Directive 2005/36/EC, for recognition of

[62] EFTA Surveillance Authority, 'Letter of formal notice to Norway concerning the lack of compensation measures for the recognition of health professionals, in particular nutritionists, in Norway' (September 2024) <https://www.eftasurv.int/cms/sites/default/files/documents/gopro/Case%2091996%20College%20Decision%20152%2024%20COL%20-%20Letter%20of%20formal%20notice%20-%20Norway%20-%20Lack%20of%20compensation%20measures%20for%20the%20r.pdf> accessed 1 September 2025.

[63] Directive 2005/36/EC (n 22) Articles 13 and 14.

[64] EFTA Surveillance Authority, 'Letter of formal notice to Norway concerning the lack of compensation measures for the recognition of health professionals, in particular nutritionists, in Norway' (September 2024) <https://www.eftasurv.int/cms/sites/default/files/documents/gopro/Case%2091996%20College%20Decision%20152%2024%20COL%20-%20Letter%20of%20formal%20notice%20-%20Norway%20-%20Lack%20of%20compensation%20measures%20for%20the%20r.pdf> accessed 1 September 2025.

qualifications of health professionals, it is allowed to require knowledge of the local language. Nevertheless, language requirements should not go far beyond what is necessary to attain the objective of the profession or posting;

4) Applicants who do not meet recognition requirements under Directive 2005/36/EC can still pursue a regulated profession in the host State by relying on Articles 28 and 31 EEA.[65]

The legislative framework, judicial interpretation and enforcement measures reveal a complex but incomplete realization of mutual recognition and homogeneity. This calls for closer coordination and reform, as will be outlined in the closing section.

4 FINAL REMARKS

In conclusion, health professionals in the EU and EEA who seek to exercise their freedom of movement have to overcome various barriers in order to access labour markets. These barriers hinder an effective application of the principle of mutual recognition, but in some cases, they can be justified on grounds of patient safety. Nevertheless, the EFTA Court has set a series of rules that seek to protect free movement of health professionals in the EEA and EU internal order.

A key reason why barriers persist within the internal market lies in the different perspectives underpinning EU and EEA law in relation to national law. From the EU's perspective, and consequently the EEA's perspective, health professionals are economic actors exercising their rights to free movement.[66] On the other hand, national regulations are often based on social considerations such as patient safety, public interest and ensuring the sustainability of national health systems.[67] As the legal literature has noted, this duality highlights the complexity of integrating health services within the internal market.[68] For example, this problem between economic integration and public health protection is not unique to professional mobility and the recognition of professional qualifications. Similar issues have risen in the CJEU's case law on cross-border healthcare, when balancing patients' free movement rights against Member States' responsibilities to organise effective health

[65] As has been mentioned in Case E-3/20 of the EFTA Court (n 56), 'an assessment under Articles 28 and 31 EEA is not the same as the assessment for recognition of professional qualifications under the Directive. Therefore, it is neither necessary nor sufficient to demonstrate that the completed training in the home State fulfills the minimum training conditions laid down in the relevant provisions of the Directive. However, the Court considers that if an applicant has received training that satisfies the minimum training conditions specified in the Directive, that should simplify and facilitate the comparison of the qualifications obtained by the applicant with the requirements in the host State'.

[66] The understanding of workers or the self-employed as economic operators within the EU stems from the interpretation of the CJEU, when the aforementioned individuals are engaged in an economic activity to exercise their free movement rights. See for example Case C-55/94 Gebhard (n 54); Case 139/85 *R H Kempf v Staatssecretaris van Justitie* EU:C:1986:223; Case 66/85 *Deborah Lawrie-Blum v Land Baden-Württemberg* EU:C:1986:284.

[67] Mike Saks, 'The Regulation of Healthcare Professions and Support Workers in an International Context' (2021) 19 Human Resources for Health 74.

[68] For more information the following readings are recommended: Tamara K Hervey, 'The European Union's Governance of Health Care and the Welfare Modernization Agenda' (2008) 2(1) Regulation & Governance 103; Tamara K Hervey and Jean V McHale, 'Law, Health and the European Union' (2005) 25(2) Legal Studies 228; Tamara K Hervey and Bart Vanhercke, 'Health Care and the EU: The Law and Policy Patchwork' in Elias Mossialos et al (eds), *Health Systems Governance in Europe: The Role of EU Law and Policy* (Cambridge University Press 2010).

systems.[69]

However, health professionals who have obtained their qualifications within the EU or EEA should not be forced to rely on judicial intervention to exercise their profession in another MS. Addressing this issue requires more effective inter-institutional cooperation, especially between national ministries of employment and education at the Union level. Such cooperation is essential not only to ensure that educational programs across MS align with the demands of the evolving labour market, but also to harmonize qualification standards for regulated professions. This would facilitate the free movement of persons and uphold the principle of mutual recognition in line with the principle of homogeneity. Attention should be drawn to the barriers faced by undertakings and individuals in liberal professions when exercising the freedom to provide services, particularly in securing recognition of their professional qualifications on a temporary basis. This is an area in which further research is required.

To end with, health personal mobility should be analysed within the broad strategies directed to the workforce in Europe.[70] The labour market must be understood as intrinsically linked to the education system, especially in the context of rapid digital transformation, which constantly generates demand for new skills and professional profiles. In the absence of coordinated efforts to align educational curriculums with labour market needs, there is a growing risk of producing outdated qualifications and exacerbating the widening gap between the EU and EEA systems, undermining the success of the internal market.

[69] For example in Case C-158/96 *Kohll v Union des caisses de maladie* EU:C:1998:171, the CJEU stated that 'Community law does not detract from the powers of the Member States to organise their social security systems, they must nevertheless comply with Community law when exercising those powers'.
[70] Buchan et al (n 6).

LIST OF REFERENCES

Barnard C, *The Substantive Law of the EU: The Four Freedoms* (7th edn, Oxford University Press 2022)
DOI: https://doi.org/10.1093/he/9780192857880.001.0001

Buchan J et al (eds), 'Health Professional Mobility in a Changing Europe: New Dynamics, Mobile Individuals and Diverse Responses' (European Observatory on Health Systems and Policies, WHO 2014) <https://iris.who.int/handle/10665/326372> accessed 1 September 2025

Fredriksen HH and Franklin CNK, 'EEA Law and the EU Internal Market: A Growing Tension' (2015) 52 *Common Market Law Review* 629
DOI: https://doi.org/10.54648/cola2015049

Hervey TK and McHale JV, 'Law, Health and the European Union' (2005) 25(2) Legal Studies 228
DOI: https://doi.org/10.1111/j.1748-121X.2005.tb00614.x

Hervey TK and Vanhercke B, 'Health Care and the EU: The Law and Policy Patchwork' in Elias Mossialos et al (eds), Health Systems Governance in Europe: The Role of EU Law and Policy (Cambridge University Press 2010)
DOI: https://doi.org/10.1017/CBO9780511750496.003

Hervey TK, 'The European Union's Governance of Health Care and the Welfare Modernization Agenda' (2008) 2(1) Regulation & Governance 103
DOI: https://doi.org/10.1111/j.1748-5991.2007.00028.x

Horspool M, Humphreys M, and Wells-Greco M, *European Union Law* (10th edn, Oxford University Press 2018)
DOI: https://doi.org/10.1093/he/9780198818854.001.0001

Kellerbauer M, Klamert M, and Tomkin J (eds), *The EU Treaties and the Charter of Fundamental Rights: A Commentary* (Oxford University Press 2019)
DOI: https://doi.org/10.1093/oso/9780198794561.001.0001

Page EC, 'The European Union and the Bureaucratic Mode of Production' in Menon A and Wright V (eds), *From the Nation State to Europe: Essays in Honour of Jack Hayward* (Oxford University Press 2001)
DOI: https://doi.org/10.1093/0199244030.003.0009

Saks M, 'The Regulation of Healthcare Professions and Support Workers in an International Context' (2021) 19 Human Resources for Health 74
DOI: https://doi.org/10.1186/s12960-021-00618-8

INTERVIEW

Notes on the Political Economy Of Green Transition: A Conversation with Ioannis Kampourakis

Alezini Loxa,* Mahesh Menon† And Ioannis Kampourakis‡

This article presents a conversation with Dr. Ioannis Kampourakis, Associate Professor of Law and Markets at Erasmus University Rotterdam, as part of Lund University's Screening for Sustainability project. Kampourakis' research explores the political economy of the green transition, focusing on how markets can be deliberately designed and steered – what he calls 'market instrumentalism' – to achieve sustainability goals. Drawing on Kampourakis' research, Dr. Alezini Loxa and PhD candidate Mahesh Menon enter into a conversation about the political economy of green transition with a focus on the European Green Industrial Policy. They discuss with Kampourakis about the changing role of law in relation to state capitalism, the potential for democratic control over the green transition, the challenges that arise for countries in the Global South as well as the recent political backlash both in the EU and in the US to sustainability related policies.

1 INTRODUCTION

As part of a strategic commitment to bettering the world through knowledge and innovation, Lund University is home to many projects on sustainability..[1] At the Faculty of Law, one such project is the Screening for Sustainability project, led by Dr. Daria Davitti and funded by Formas.[2] As part of this project, Post-Doctoral Research Fellow Alezini Loxa and PhD Researcher Mahesh Menon initiated a conversation with Dr. Ioannis Kampourakis, Associate Professor of Law and Markets at Erasmus University, Rotterdam on the political economy of green transition.

Kampourakis' scholarship focuses on examining the intersection of law, markets and economic planning, particularly in the context of sustainability transitions and post-neoliberal economic arrangements. A central thesis in Kampourakis' work is what he terms 'market instrumentalism' – the idea that markets can be deliberately structured and deployed as tools for achieving political objectives, rather than being treated as neutral or natural mechanisms. Through detailed analysis of policies like the EU Green Industrial Plan and China's New

* NYU Emile Noel Fellow 2025-2026 and Post-Doctoral Research Fellow in EU Law, Lund University.

[1] For more information see <https://www.lunduniversity.lu.se/about-university/university-glance/mission-vision-and-values/sustainability> accessed 1 September 2025. Among the projects special mention should be made to the Agenda 2030 Graduate School established in 2018 in order to bring together PhD students across all disciplines who work on sustainability related questions. Alezini Loxa completed her Ph.D as a part of the Graduate School while Mahesh Menon is a currently a Ph.D candidate within it.

[2] For more information, see <https://screeningforsustainability.org/> accessed 1 September 2025.

Energy Vehicles Strategy, he demonstrates how markets are increasingly being shaped to serve specific public purposes, particularly in sustainability transitions.[3]

Perhaps his most innovative contribution is his analysis of how planning can occur within market frameworks. He challenges the traditional dichotomy between markets and planning, arguing that all markets involve some degree of planning through their legal and institutional architecture. His work demonstrates how varying degrees of central coordination can exist within market economies. Moreover, his work provides us with important theoretical tools for understanding how legal and institutional frameworks can be reshaped to address sustainability challenges while acknowledging the continued reality of market economies.

Central in Kampourakis' work is the argument that there are alternatives beyond pure market solutions and complete state control, offering practical insights for policymakers and theorists alike. It should thus come as no surprise that we wanted to engage more closely in his work as part of the Screening for Sustainability Project, whose purpose is to bring together experts in order to exchange ideas and collectively understand the legal complexity behind various frameworks adopted with a view to promoting sustainability in Europe and beyond. In what follows you will find the conversation we had with Ioannis during an afternoon in late February 2025.[4] We hope that our discussion will enrich the ongoing debate on the political economy of green transition.

2 EU LAW AS AN INSTRUMENT OF MARKET PLANNING

Alezini Loxa: Before going deep into your theoretical contributions, could you briefly explain to our audience what the European Green Industrial Policy is?

Ioannis Kampourakis: Yes, of course. The European Green Industrial Policy refers to the set of policies the EU is deploying to reshape its economy and, more narrowly, its industrial production in line with its climate and sustainability objectives. Its goal is to promote 'green growth', while also ensuring the resilience and competitiveness of the EU economy in times of increasing geopolitical competition. In fact, recently, EU politics may be tilting the balance more toward competitiveness and resilience and less towards greening.

In any case, the key components of EU Green Industrial Policy have so far been the Critical Raw Materials Act, which seeks to secure access to essential minerals for the green and digital transition and thus to reduce reliance on external suppliers; the Net-Zero Industry Act, which aims to boost domestic clean tech manufacturing; the Chips Act, which seeks to enhance domestic semiconductor production, again with a goal of resilience and reducing external dependence; and, finally, the recent Clean Industrial Deal, which seeks to 'make

[3] See European Commission, 'Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, A Green Deal Industrial Plan for the Net-Zero Age' COM(2023) 62 final; State Council of PRC, 'New Energy Vehicle Industry Development Plan (2021-2035)' (2020)

[4] For the video version, see <https://www.youtube.com/watch?v=wIYWZgY4sHk> accessed 1 September 2025.

decarbonization profitable' by facilitating industrial access to energy.[5] Of course, these Acts are complemented by the broader, ongoing legal developments and shifting EU priorities – for example, the loosening of state aid rules, the development of green financing mechanisms, such as the InvestEU program, or the use of trade instruments like the Carbon Border Adjustment Mechanism to shield domestic industries from external competition.[6]

Alezini Loxa: In light of the importance of the European Green Industrial Policy Plan for the EU's sustainability aspirations, you suggest that there is a shift in the function of law in the EU integration process and, relatedly, in the relation of law to market planning. Would you want to unpack how law has been used as an instrument to safeguard market competitiveness in the past?

Ioannis Kampourakis: Indeed, I argue that, to some extent (and only to some extent), the Green Industrial Policy Plan signals a certain conceptual shift from the neoliberal paradigm of EU economic regulation, which was defined by the commitment to the safeguarding of the competitive market order. As critical literature has shown, the function of the law in the neoliberal paradigm has been to insulate the sphere of market exchange from political contestation and democratic renegotiation.[7] In the context of the EU, this has happened, indicatively, through the enshrinement of market freedoms as quasi-constitutional principles, the judicial enforcement of market primacy against national regulations, strict state aid rules and the use of competition law to prevent government intervention in markets, the development of an autonomous monetary policy committed to price stability or hard fiscal constraints that depoliticize economic policy.

Beyond this 'encasing' function, the role of law has also been to embed within public power a kind of neutrality towards 'value' and social need – 'what should be produced?', 'where should we be investing as societies?' – understanding such 'value' as something that may only be determined through market competition. In other words, neoliberalism meant a reorientation of the state from the production of a mystified 'social value' (after all, who would be legitimated to decide about it?) to the safeguarding of the competitive process, where market value is the only authoritative measure of value and need. This shaped a form

---

[5] Regulation (EU) 2024/1252 of the European Parliament and of the Council of 11 April 2024 establishing a framework for ensuring a secure and sustainable supply of critical raw materials and amending Regulations (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1724 and (EU) 2019/1020 [2024] OJ L2024/1252; Regulation (EU) 2024/1735 of the European Parliament and of the Council of 13 June 2024 on establishing a framework of measures for strengthening Europe's net-zero technology manufacturing ecosystem and amending Regulation (EU) 2018/1724 [2024] OJ L2024/1735; Regulation (EU) 2023/1781 of the European Parliament and of the Council of 13 September 2023 establishing a framework of measures for strengthening Europe's semiconductor ecosystem and amending Regulation (EU) 2021/694 (Chips Act) [2023] OJ L229/1; European Commission, 'The Clean Industrial Deal: A joint roadmap for competitiveness and decarbonisation' COM(2025) 85 final.

[6] Regulation (EU) 2021/523 of the European Parliament and of the Council of 24 March 2021 establishing the InvestEU Programme and amending Regulation (EU) 2015/1017 [2021] OJ L107/30; Regulation (EU) 2023/956 of the European Parliament and of the Council of 10 May 2023 establishing a carbon border adjustment mechanism [2023] OJ L130/52.

[7] Indicatively, see Quinn Slobodian, *Globalists: The End of Empire and the Birth of Neoliberalism* (Harvard University Press 2018); Fritz W Scharpf, 'The Asymmetry of European Integration, or Why the EU Cannot Be a "Social Market Economy"' (2010) 8(2) Socio-Economic Review 211.

of statecraft that leaned on claims of neutrality, cost-efficiency or proportionality to facilitate and safeguard a political project that prioritized market ordering.

3 BEYOND THE MARKET-PLANNING BINARY: RETHINKING STATE CAPITALISM AND GREEN INDUSTRIAL POLICY

Mahesh Menon: You argue that law makes planning possible not just beyond but also within markets. What do you mean by this, and how does your analysis of new energy vehicle policies in China, the EU and US illustrate this point?

Ioannis Kampourakis: My point here is that markets, as products of human design, may be used to serve politically set objectives – functioning, in a way, as instruments of planning. In some ways, this speaks to models of state capitalism or forms of indicative planning, where the state does not simply regulate or correct markets; rather, it actively plans *within* markets to steer economic activity toward strategic objectives.

The case of electric vehicles shows how targeted legal interventions that reshape the rights and duties of different actors in the economy can achieve a very specific political objective – the development and wide adoption of a particular technology (regardless of what we think about electric vehicles per se and whether this is a worthy goal). Such planning is necessarily a patchwork exercise: for example, in the case of electric vehicles in China, it required subsidies and investment in research and development, monetary incentives for consumers, conditionalities for locally produced batteries and public procurement, change of traffic restrictions and regulatory controls around vehicle ownership, targeted opening of foreign investment and, ultimately – once the design of industrial policy has borne fruit and production of electric vehicles has been upscaled – the transitioning to market competition without government support so that only the most competitive electric vehicles survive. That means that even market competition may be used instrumentally as a disciplinary force to achieve certain political objectives. Judging by the results, the Chinese experience in the electric vehicle sector has been a success both in quantitative and in qualitative terms. If you watch some early videos of Elon Musk talking about BYD cars – back in the early days of the industrial policy I just described – he laughs and mocks their quality. Now BYD has surpassed Tesla in global EV sales.[8]

Mahesh Menon: Your work suggests we need to analyse planning as occurring on a spectrum rather than as a binary choice between markets and planning. Could you explain this spectrum approach and its implications for understanding different modes of economic coordination?

Ioannis Kampourakis: Planning as a spectrum starts from the assumption that the economy is necessarily, to a significant degree, a product of deliberate design. Any kind of allocation of legal entitlements (e.g. the scope of property rights or contractual freedom) is political and is bound to have distributive effects. From this perspective, we could think of market design as planning in a spectrum – or, perhaps better, a continuum – rather than

[8] See Sam Meredith, 'Chinese EV giant BYD outpaces Tesla with annual sales of more than $100 billion' (*CNBC*, 25 March 2025) <https://www.cnbc.com/2025/03/25/ev-giant-byd-outpaces-tesla-with-annual-sales-of-over-100-billion.html> accessed 1 September 2025.

a binary choice. At the one end of the spectrum we can place the full entrustment of coordination of production and investment to business and private decision-making, with the state restricting itself to guaranteeing property rights, competition rules and price stability. This concentrates political coercion and expands market coercion. If we exclude command-type economies and keep the analysis within capitalist parameters, at the other end of the spectrum we can place forms of state capitalism with state ownership and strong state disciplinary power towards capital and market actors. In this case, we see a maximization of political coercion and a more flexible approach toward market coercion. In between, planning within capitalism involves different degrees of public and conscious shaping of economic activity in the pursuit of political and social objectives.

This kind of analysis allows us to demystify the notion of state 'intervention' in a supposedly naturalized economy. Instead, any design of the economy can be conceptualized as a specific allocation of rights and duties of different actors. When the state 'intervenes', it simply restructures those rights, favouring some actors as opposed to others.

Alezini Loxa: In discussing green industrial policy, you argue that the market can function as an instrument of planning while acknowledging certain structural limits. Can you discuss what these limits are? What do you see as the key opportunities and constraints of using markets as tools for sustainability transitions?

Ioannis Kampourakis: My argument starts from the assumption that – despite their institutional, human-made dimension – markets have certain essential properties; for instance, they are made up of exchange-based transactions that are done for individual gain. These properties entail a predilection to produce certain kind of effects. If the profit motive, for example, is an essential property of markets, this means that all market-based institutional formations will be permeated by it. This does not necessarily neutralize the functional and coercive power of market processes, as the profit motive may itself be instrumentalized as part of industrial policy design. However, it concedes significant ground when it comes to broader visions of social transformation. The reliance on the profit motive means that no effort is made to seek the foundations of new motivations and overcome the alienation of individuals from each other, from society and from nature.

But even in the narrower context of sustainability transitions, the profit motive proves incompatible with goals of socio-ecological transformation. For example, in the recent book *The Price Is Wrong*, economic geographer Brett Christophers shows how private investment in solar energy is simply not profitable enough unless it is publicly subsidized.[9] This means that sustaining a private-led sustainability transition requires the state to constantly subsidize private accumulation – which ultimately forecloses the social dimension of sustainability transitions. In addition, relying on profit-driven private initiative generalizes the market logic of cost-efficiency, which, in itself, detracts from sustainability objectives, if we think about goals such as durability, conservation, etc. Finally, the profit motive means that private actors are likely to cherry-pick the aspects of industrial policy that offer quick returns. For example, green industrial policy initiatives in the US have led to investment in the most short-term profit possibilities – electric vehicles – rather than into the full range of new technologies

[9] Brett Christophers, *Price is Wrong: Why Capitalism Won't Save the Planet* (Verso 2024).

that would be required for a green transition. This, in turn, reinforces historical patterns of unequal ecological exchange and extractivism that are socially and environmentally destructive – just think of all the new mining projects for critical raw materials.

4 MARKET INSTRUMENTALISM, POLITICAL CAPITALISM AND DEMOCRATIC CONTROL IN THE GREEN TRANSITION

Mahesh Menon: Your framework emphasizes the potential for democratic control over the economy through market instrumentalism. However, given the transnational nature of capital and production networks, isn't there a risk that this potential remains largely theoretical without radical transformations?

Ioannis Kampourakis: Market instrumentalism conveys a promise that markets may be used to advance political and social objectives. In that sense, it conveys an assertion of collective self-determination over what is often presented as natural, apolitical, anonymous market processes. However, following up on the previous answer, what the strategic deployment of markets can achieve is limited. One reason is that the reliance on private ownership and profit-based initiative inherently constrains the scope of state intervention, as the logic of capital accumulation imposes structural imperatives that shape both the state's options and the outcomes of its interventions. Nevertheless, this is not to say that the scope of private ownership and profit-based initiative cannot be constrained even *within* conditions of capital accumulation – but this would require further analysis.

Another reason for the limitations of market instrumentalism, as you point out, is that state control would have to function in a context of transnational circuits of capital. Capital mobility limits the ability of any single state to impose binding constraints on capital. Yet, there are some counterpoints here as well: capital mobility itself can be restrained, trade and investment agreements can be redrawn, and market instrumentalism can involve public ownership (not only private investment). In short, while I agree with your point that the transnational nature of capital places limits on state-led projects to democratize the economy, it is worth reflecting on the extent to which the 'transnational nature of capital' is itself a product of state power – and, therefore, potentially reversible.

Alezini Loxa: In your recent work, you develop a dual thesis of 'market instrumentalism' and 'political capitalism' to analyse emerging legal rationalities in the EU green industrial policy. Could you explain what these two concepts mean, how they work together and what they reveal about the changing role of law in the path to green transition?

Ioannis Kampourakis: By referring to 'market instrumentalism' in the context of EU green industrial policy, I mean the emergence of a regulatory regime that casts off its agnosticism about value that I described earlier and, thus, the commitment to competitive markets *in the abstract*. In contrast to the model of neoliberal statecraft that delegated authority to market ordering and relied on processes of market coordination not only for welfare and social prosperity but for the very definition of that 'welfare' and 'prosperity', the new economic statecraft launched by EU green industrial policy reaffirms – even if half-heartedly – the role

of the political in the economic order. What emerges is a regulatory regime that seeks to shape markets in alignment with politically determined objectives. The attempt to design markets that generate social effects in line with political priorities introduces a concept of value that is *external* to the market and the competitive order. This interjection of 'social value' through the establishment of meta-objectives, like climate neutrality, reflects an ongoing, incomplete transition from market coordination to political coordination.

By using 'political capitalism', I attempt to capture how the legal architecture of the green transition introduces a form of statecraft that does not only seek to secure the conditions for private accumulation but rather becomes actively involved in it. This challenges the idea of public power as a depoliticizing force that only insulates markets, which I also briefly described before. What we see instead is that public power politicises private accumulation – most notably through strategies of derisking that guarantee private profitability and socialise the risks of investment. Political capitalism complements market instrumentalism; the reconceptualisation of markets as instruments for political ends presupposes a redefined role for public power in economic statecraft to sustain an economy rooted in profit and private ownership over the means of production. In other words, the willingness to deploy markets for political ends is coupled with the direct involvement of public power in value formation and the securing of private accumulation in ways that signal a changing, 'post-neoliberal' state-market relation.

5 FROM POST-NEOLIBERAL POSSIBILITIES TO GLOBAL JUSTICE CHALLENGES.

Mahesh Menon: Your analysis draws heavily on EU and Chinese examples of industrial policy. To what extent do you think your conclusions about post-neoliberal possibilities can be generalized given the unique institutional contexts of these cases?

Ioannis Kampourakis: In answering questions like this, we have to take into account factors like path dependency, institutional specificity as well as other contingent factors, like societal pressures, labour organisation and mobilisation, etc. Any discussion of the state in capitalism has to be a historically situated analysis that examines the particular, historically specific regime of accumulation. That said, I believe the themes of *market instrumentalism* and *political capitalism* capture a broader and evolving trend: the deepening entanglement of public power with processes of capital accumulation. This trend is particularly visible in the growing role of the state in *derisking* private investment – acutely observed by economic geographers in the renewables sector – and reflects a shift toward more proactive forms of administering accumulation. It is also important to remember that the debate around *political capitalism* originally emerged in the United States, particularly as part of intra-left critiques of the so-called 'Bidenomics'. Still, any shift beyond neoliberalism remains contested and uneven and it is bound to take different shapes depending on the institutional context.

Mahesh Menon: You argue for combining strategic market deployment with expanded decommodification. But given the tendency of market rationalities to

colonize other social spheres, isn't there a danger that this hybrid approach ultimately reinforces rather than transforms market dominance?

Ioannis Kampourakis: This is a great and challenging question. On a first level, this is indeed one way to see it, and I mostly agree with the critical point. Strategic market deployment is another way of perpetuating – and potentially even rescuing or reinforcing – the capital relation. This insight resonates with various critical traditions of political economy, including the Frankfurt School and the Regulation School. This is also what I tried to show with the idea of 'political capitalism' and the shifting institutional forms that enable accumulation. This kind of commitment to accumulation will likely erode the very bases of decommodification in the long term, if not make them impossible from the outset. Yet, there are two potential challenges or complications that I believe are worth reflecting on in more detail.

One challenge has to do with temporalities. If the starting point is a capitalist economy operating on the basis of the profit motive and private ownership over the means of production, then it is difficult to see how to transition directly to a fully decommodified society. In that sense, market instrumentalism (and the form of state control over the economy it implies) could be a transitory stage, creating public capacity for advancing decommodification. Of course, this strategic approach would need to be coupled with directly decommodifying and redistributive measures. In a way, such an approach resonates with early visions of social democracy that saw state intervention not as a correction of 'market failures' but as intermediary steps and a transition mechanism towards a post-capitalist society.

Another challenge has to do with what your critical point presupposes: that is, the market tendency to colonize other social spheres. Even if we agree that this tendency is an essential property of markets, should we really understand it as an unyielding force? Or is this being overly deterministic? To what extent could this tendency of colonization be contained – for example by institutions and societal pressures? While there are no easy answers here, China's experience indicates that there might be avenues – even if historically and politically specific – to maintain the primacy of the political and forms of discipline toward private capital, in ways that precisely contain this colonizing tendency. Similarly, drawing from examples of industrial democracy and the welfare state in post-war Europe, we can think of the kind of societal counterpowers, such as organized labour, that can achieve a similar containing effect.

Alezini Loxa: When we think about green industrial policies and the drive for strategic autonomy in the Global North, what implications do you see for Global South countries? How might the legal frameworks you analyse need to be rethought when considering questions of global justice, particularly given existing patterns of global production and resource extraction?

Ioannis Kampourakis: This is an important dimension of the discussion. The EU's pursuit of domestic green growth, in particular through the emphasis on critical raw materials, clearly risks perpetuating and reinforcing existing patterns of core-periphery extractivism. Your reference to strategic autonomy is well placed. The EU has leveraged WTO law to challenge export restrictions and developmental strategies of resource-rich countries, such as

Indonesia. At the same time, it has negotiated free trade agreements that prohibit export taxes, export monopolies, dual-pricing etc. while securing market access for European investors. There is growing literature on how the EU's greening aspirations fit within a historical continuum of colonial and neo-colonial relations.[10] Of course, EU industrial policy was never about global justice to begin with. But even if we take its nominal goal of climate neutrality seriously, then the continuation of extractivism and the exacerbation of global inequalities and unequal ecological exchange for *domestic greening* is short-sighted and counterproductive.

There is an argument that mining is essential for green technologies and, thus, for a green transition, with EU regulations aiming to mobilize extraction projects not only abroad but also within the Union. Yet this push raises a set of questions and public debates that have, so far, been insufficiently addressed: 'How much mining is truly necessary?', 'For which technologies or commodities?'. For instance, should electric cars be prioritized, or should we focus more on expanding public transportation? The answers to questions about production and investment priorities also determine the volume of mining required for a 'green transition'. Similarly, how should profits associated with mining projects be distributed – and to whose benefit? We know that export of raw cobalt and lithium constitutes only about 0.6% of the total value chain – this effectively locks extraction sites into a subordinate position, confined to the low-value end of the chain, with the bulk of profits accruing further downstream. Finally, what role do affected communities play in the decision-making? For example, while the European Parliament introduced amendments to the Critical Raw Materials Act aimed at protecting indigenous rights – including provisions for meaningful consultation and fair compensation – these safeguards remain weak when measured against the well-documented and recurring patterns of extractive exploitation.

6 BETWEEN DEMOCRATIC PROMISE AND POLITICAL BACKLASH

Mahesh Menon: After the recent US election, different EU political actors have suggested that simplification and deregulation might be the key to ensure the competitiveness of European markets.[11] The relevant statements, together with the proposal for an EU Omnibus as a means to revisit the commitments agreed in the Corporate Sustainability Reporting Directive the Corporate Sustainability Due Diligence Directive and the EU Taxonomy has created a lot of concern within Business and Human Rights circles about the possibility of backtracking the commitments made in the European Green Deal.[12] What is your opinion on these evolutions?

---

[10] See Diana Vela Almeida and others, 'The "Greening" of Empire: The European Green Deal as the EU first agenda' (2023) 105 Political Geography 102925; Sanja Bogojević, 'The European Green Deal, the rush for critical raw materials, and colonialism' (2024) 15(4) Transnational Legal Theory 600.

[11] See also Report by Mario Draghi, 'The future of European competitiveness' (September 2024, Publications Office of the European Union 2025).

[12] European Commission, 'Proposal for a Directive of the European Parliament and of the Council amending Directives (EU) 2022/2464 and (EU) 2024/1760 as regards the dates from which Member States are to apply

Ioannis Kampourakis: I have also followed these developments. Indeed, there does seem to be growing opposition against the Green Deal, both from the European far-right and – crucially – from the center-right, which is to some extent ironic, because the Green Deal is very much a product of the political right and, one could say, even a core legacy of von der Leyen. As we briefly discussed before when we referred to 'political capitalism' (and despite the more theoretical point of a conceptual shift), the Green Deal does not decisively break with neoliberal economic governance, and it relies heavily on derisking private investment, which serves as a way to guarantee private accumulation. At the same time, we know that financial capital was significantly involved in the shaping of certain of its aspects, such as the sustainable finance agenda.

These current developments make it tempting to assume a defensive position of the Green Deal as a whole, considering that the alternative might be deregulation. However, in my opinion there is also space for a more assertive stance. This would be to reclaim the conceptual core of the Green Deal properly understood – that is, its assertion of public control over the economy and the setting of climate neutrality as a political target – while redesigning its policy tools to *expand* public capacity and strategic direction. That means moving beyond derisking toward direct public investment, toward further democratization of industrial policy – for instance through the expansion of public ownership and the creation of Investment Boards – and toward the introduction of meaningful constraints on private capital, such as restricting exit from green investments rather than merely subsidizing them. Even if such an agenda is only partially successful, this is the kind of effort that could potentially pull the political centre of gravity and influence the fate of the Green Deal.

7 LOOKING INTO THE FUTURE

Alezini Loxa: Finally, in a utopian scenario, where you have full control over the direction of the political economy of green transition in the EU, what measures would you pursue?

Ioannis Kampourakis: This is a generous offer! If we are talking about full control, I think we need to look beyond concrete policies, to the forms of public power that underpin an economy revolving around profit. My normative thinking is built around three forms of power: public decision-making power, disciplinary power, and countervailing power. Decision-making power is the most far-reaching. Essentially, it calls for expanding democratic decision-making over the allocation of productive and investment resources. It means we should have a say, as citizens, over the direction of the economy: over what is produced, what has value for our societies, where our resources are invested, etc. Of course, there are different ways such public decision-making power could manifest – for example, through public ownership, state-controlled finance, public investment based on decisions by

certain corporate sustainability reporting and due diligence requirements' COM(2025) 80 final; European Commission, 'Proposal for a Directive of the European Parliament and of the Council amending Directives 2006/43/EC, 2013/34/EU, (EU) 2022/2464 and (EU) 2024/1760 as regards certain corporate sustainability reporting and due diligence requirements' COM(2025)81 final

investment boards, etc. In its core, this is a form of power that calls for restricting the domain of the market and expanding collective self-determination over the economy.

Your question gave me full control, so I could stop here. But for the sake of completion, let me say something about the other two forms of power I mentioned. Disciplinary power is envisioned within a context of market economy and refers to how the state can discipline private actors, expanding an arsenal of control measures aimed to ensure the alignment of private activity with public goals. These could include, for example, measures such as capital controls, buffer stocks, price controls or limits on early exit from green investments.

Finally, countervailing power is a corrective to the centralizing tendencies of the two previous directions. It is a recognition that democratizing the economy requires effective deliberation and participation in the decision-making structures, with particular attention to social groups that are structurally disadvantaged and often excluded from governance decisions. This participatory impetus could extend both in the public sector, as a counterweight to technocratic managerialism, and to the private sector, through the institutionalisation of mechanisms of dissent and self-contestation in corporate governance that may challenge the commitment to accumulation.

BOOK REVIEW

Joyce De Coninck, *The EU's Human Rights Responsibility Gap, Deconstructing Human Rights Impunity of International Organisations*, Hart Publishing 2024, 280 pages

Emiliya Bratanova*

In her book, *The EU's Human Rights Responsibility Gap, Deconstructing Human Rights Impunity of International Organisations*, based on her dissertation, Joyce De Coninck addresses a perennial question about how third country nationals (TCNs) who have been subjected to unlawful human rights conduct by the European Union (EU) can seek and obtain legal redress. In the current EU political and legal context — characterised by a migration management mode which aims to reduce the number of incoming TCNs through 'a strict application of the "in/out" dichotomy, which relies on methods of externalisation, informalisation, securitisation including militarisation, digitalisation, and agencification'[1] — De Coninck engages in an 'arduous endeavour', as she rightfully puts it.[2] Namely, she sets out to analyse the intersection between the responsibility rules applicable to the EU under EU law and international law, on the one hand, and the human rights regime under EU and international law, on the other.

Following this analysis, which spans multiple legal domains and also substantive areas of EU law, she tests the outcome of her theoretical legal framework on four practical cases in the area of integrated border management (IBM). More concretely, she tests the EU's normative commitment to the principle of *non-refoulement* in four scenarios corresponding to the 'four-tier access control model' of IBM.[3] The first scenario focuses on visa regulation under EU law, the second scrutinises the maritime operation Sophia in the Mediterranean, the third zooms in on Frontex conduct in the Aegean Sea in concert with the Greek Coastguard, and the fourth one delves into the informalisation of readmission agreements, focusing in particular on the EU-Turkey Statement.

What is unique about this book is its angle of scrutiny on the question of the human rights responsibility of the EU — which De Coninck defines as 'transversal', as opposed to unidimensional accounts of how to identify the most promising avenues for judicial redress in concrete cases of alleged human rights violations on behalf of the EU. While the latter approach does not question the existing human rights architecture of the EU, De Coninck reverses the questions posed. She is not interested in identifying the right adjudicative body and avenue *in order to* hold the EU responsible for human rights harms, but goes beyond this

* PhD Researcher, Lund University, Sweden.

[1] Joyce De Coninck, *The EU's Human Rights Responsibility Gap, Deconstructing Human Rights Impunity of International Organisations* (Hart Publishing 2024) 30.

[2] ibid Foreword, v.

[3] ibid 25 and note 70: The 'four-tier access control model' of IBM 'encompass[es] measures in third countries (1); cooperation with neighbouring countries (2), control measures at the EU border (3) and measures within EU territory including measures concerning return (4)'.

first level of analysis. What she does can be defined as a meta-analysis of whether and to what extent the existing EU human rights regime in combination with the EU's responsibility framework allows TCNs to seek and obtain redress more broadly. Her book asks whether this is possible at all. The effort put into pursuing this complex objective is tremendous. The work is very well researched, with detailed and comprehensive references and a clear structure, offering flowing text which could easily be used for instructional purposes.

The book is divided into four parts, whereby the first part introduces the chosen methodology and sets the scene, creating a sense of urgency about why the offered knowledge is not only timely, but crucial to understanding and possibly remedying the identified shortcomings of the underlying EU's human rights and responsibility legal frameworks; the second part offers a thorough legal analysis, on the one hand, of the human rights obligations of the EU and of international organisations more broadly, and on the other, of the rules establishing responsibility for the EU and for international organisations more broadly; the third part applies the findings from part II to the four scenarios pertaining to different aspects of the IBM, as outlined above; and the fourth part offers a way forward with suggestions on how to overcome the identified shortcomings.

In part I, De Coninck identifies the sources of human rights norms which govern the conduct of the EU. From the perspective of international law, the EU is guided by customary international human rights law (human rights norms) and the Articles on the Responsibility of International Organizations (ARIO) (responsibility rules). From the perspective of EU law, it is the Charter of Fundamental Rights of the EU and the EU general principles which form the EU human rights architecture. The link between the two is the right to an effective remedy, which has the status of an international customary norm.[4] In terms of approach, the author engages, firstly, in a functional appraisal of the EU's human rights responsibility regime[5] and, secondly, in a transversal and applied appraisal which combines theory and practice in the four different concretised illustrations of EU IBM mentioned above.[6] Finally, she gives an account of the IBM context in which these appraisals are tested. The latter is one of 'transnational cooperative governance' where many actors' (states, international organisations and businesses) conduct is governed by different sets of human rights rules, which results in normative misalignment thus 'mak[ing] it attractive for different actors to collaborate, as increased and diversified forms of collaboration may in effect, minimise the risk of any one of these actors being held responsible under (international) human rights law for contributions to human rights harms'.[7] The transnational cooperative governance has led to the instrumentalization of technology which serves to severe the jurisdictional link required to trigger human rights protection of TCNs before reaching EU territory, creating 'jurisdictional black holes'.[8] Moreover, IBM is an area of shared competence between the EU and the Member States (MSs), making it difficult to concretise

[4] De Coninck (n 1) 3, citing Article 8, Universal Declaration of Human Rights; William A Schabas, *The Customary International Law of Human Rights* (Oxford University Press 2021) 273.
[5] De Coninck (n 1) citing Jan Klabbers, 'The Emergence of Functionalism in International Institutional Law: Colonial Inspirations' (2014) 25(3) European Journal of International Law 645.
[6] De Coninck (n 1) 10.
[7] ibid 13.
[8] ibid 16.

ex-ante the competence division, which poses great difficulties for the attribution of unlawful human rights conduct to the EU, the MSs or both.

Substantively, the book is quite pessimistic, despite the author's genuine attempt to find a workable solution to the well-known difficulties to hold the EU responsible for human rights harms from the perspective of TCN's who try to reach the EU in search of refuge. In part II, and as illustrated in the four scenarios in part III, the book reveals serious legal design flaws, which the author refers to as 'normative and liability incongruences'. More concretely, she argues that there is normative incongruence as far as the content of the applicable human rights norms is concerned. They are not sufficiently concrete as to give rise to negative, positive, procedural and substantive obligations for the EU as an international organisation (as opposed to states). There is also incongruence with respect to liability, which manifests on two levels. On the first level, an individual faces an insurmountable number of obstacles in their attempt to hold the EU *independently* responsible for its contribution to unlawful human rights conduct. On the second level, the current responsibility rules are not designed in a way to make it feasible for the individual to hold the EU responsible *together with* state and non-state actors for human rights harms, thus foreclosing the possibility of *shared responsibility* for all implicated actors. In brief, under the current human rights responsibility framework of the EU, it is practically impossible for TCNs to successfully seek redress for suffered human rights harms on the part of the EU, either separately or together with MSs (or other actors). More regrettably, this is the case regardless of whether the harm constitutes an operational or a legislative act on behalf of the EU and, further still, regardless of whether there are explicit human rights safeguards incorporated in the relevant secondary acts governing the alleged conduct, as in the case of Frontex (scenario 3).[9]

In order to shake off any feeling of all-consuming disappointment, in the fourth and final part of the book, De Coninck puts forward a proposal for a relational human rights responsibility regime for the EU, inspired by the work of André Nollkaemper.[10] This regime denotes a departure from the traditional model of *independent responsibility* under international and EU law, thus better responding to the contemporary power dynamics characterised by EU transnational cooperative governance in the area of IBM. It also ought to concretise the human rights commitments of international organisations (and, more concretely, of the EU) into justiciable obligations. Drawing for inspiration on business and human rights law, on the one hand, and environmental law, on the other, the author suggests that concretising the *non-refoulement* commitment could take place through mechanisms such as 'due diligence, certification, impact assessments, and review mechanisms both independently and in relation to States', resulting in the development of 'common but differentiated obligations' for the EU specifically, as compared to states' obligations.[11] At various points, the author illustrates that different approaches to shared responsibility already exist in the different areas of EU law,[12] which, if applied to the adjudication of human rights harms, could yield more

[9] De Coninck (n 1) 229.
[10] André Nollkaemper, 'Shared responsibility for human rights violations: a relational account' in Thomas Gammeltoft-Hansen and Jens Vedsted-Hansen (eds), *Human Rights and the Dark Side of Globalisation – Transnational Law Enforcement and Migration Control* (Routledge 2017).
[11] De Coninck (n 1) 271.
[12] E.g. in the area of data protection, citing Case C-755/21 P *Marián Kočner v Europol* EU:C:2024:202, where the CJEU accepts that a system of joint and several liability applies, as compared to the cases CJEU (General

promising results for redress from an individual TCN perspective. The fact that this has not happened points to the deliberate choices made by the CJEU to eschew the EU from responsibility for contributions to unlawful human rights conduct, especially as regards TCNs in the area of IBM. This is confirmed by De Coninck's observation that:

> the very loopholes, inconsistencies, and legal lacuna which characterise the EU's human rights responsibility framework and that of [international organisations] more generally, form an excellent breeding ground for the design of a border management system that instrumentalises these very drawbacks to construct a regime that in its very architecture pursues an anti-human rights agenda in its effects.[13]

However, De Coninck cannot put up with such a conclusion, and she even attempts to assess the possibility of holding the CJEU, as a body of the EU, accountable for alleged human rights violations, thus incurring independent or shared responsibility for internationally wrongful acts. This is explicitly so in scenario 1 (discussing visa regulation)[14] and implied in scenario 4 (discussing the EU-Turkey Statement).[15] This is perhaps simply a desperate act of hope, as it seems a non-starter, because there is no higher appellate court which could establish that the CJEU has erred on points of law and fact.

In the end, despite the concerningly repetitive analysis in the four different scenarios,[16] all of which resulting in the impossibility to establish responsibility for unlawful human rights conduct by the EU, the author does not espouse the 'end of human rights' paradigm,[17] despite the serious legal flaws revealed in the EU legal architecture of human rights and responsibility. Instead of engaging with critical legal theory and TWAIL approaches, De Coninck aims to go beyond critique and to offer a glimpse of optimism by following up on the book's findings. Consequently, she is currently working on substantiating and delimiting the scope of the relational human rights responsibility framework of which she is a proponent.

Court) T-600/21 *WS and Others v Frontex* EU:T:2023:492 and Order in Case T-136/22 *Hamoudi v Frontex* EU:T:2023:821.

[13] De Coninck (n 1) 265.

[14] ibid 183ff.

[15] ibid 249.

[16] As De Coninck notes herself, ibid 245.

[17] ibid Foreword vi.