The "Governance Turn" in EU Digital Policy:

The Regulatory Instruments for Regulating AI and Digital Services

Simona Stockreiter*

Contents

* Simona Stockreiter is a researcher at Hertie School, affiliated to the Jacques Delors Centre.

University of Vienna Law Review, Vol. 9 No 3 (2025), pp. 140-168, https://doi.org/10.25365/vlr-2025-9-3-140.

I. Introduction

EU digital policy legislation has evolved steadily over the last 20 years in response to the rapid development of digitalisation. In order to obtain the EU's sovereignty to decide its own fate in the era of big data, hyperconnectivity and AI, a new phase of digital policy legislation is currently being introduced. The aim of this paper is to examine which regulatory instruments are used to address the increasing regulatory challenges and to critically evaluate whether these instruments can strike a balance between the different prevalent regulatory goals, which are under growing tension: the goal to stimulate innovation and competitiveness – the goal to protect a long list of fundamental rights – and the goal to prevent foreseeable collective and societal harm.

To provide an understanding for the main regulatory orientations and tools in EU digital policy legislation, a brief historical overview of the most relevant developed legal frameworks will be presented in a first step, with a focus on data and content. In a second step, the regulatory approaches of the two current main legislative frameworks: the Artificial Intelligence Act (AI Act) and the Digital Services Act (DSA) will be analysed, and the problems of the chosen regulatory instruments will be discussed. The hypothesis being examined is that although there are clear efforts in the regulatory frameworks to strike a balance between the different regulatory goals, their regulatory instruments are not sufficient or suitable to achieve this aim. Given the foundation of both regulations in particular on internal market law, the regulatory tools utilised are unable to adequately address the complex ethical, societal, and human rights impacts of the digital transformation. Instead, there remains significant room for manoeuvre of tech companies. Subsequently, solutions for improving the current approaches are briefly proposed.

The work is based on a qualitative analysis of the two legal frameworks. In addition, a series of 16 expert interviews with officials of the European Commission, experts and civil society representatives were conducted in Brussels to provide a more profound understanding of the laws and the challenges they pose, as well as to gain insight into the discourses within the "EU Bubble".

II. Key Elements of the Evolution of EU Digital Policy

From a meta-perspective of EU digital policy-making since 2000, it can be seen that EU digital policy can essentially be divided into three phases:

University of Vienna Law Review, Vol. 9 No 3 (2025), pp. 140-168, https://doi.org/10.25365/vlr-2025-9-3-140.

The first phase is characterised by a "hands-off approach" to digital regulation.[1] The key legislative framework of this phase is the 2000 e-Commerce Directive[2], which has served for the following twenty years as the general framework for regulating digital services. Its core principles are the limited liability of intermediary services[3] and the country-of-origin principle[4]. Together with the 2006 Services Directive[5], it aims to remove legal obstacles which make "the exercise of freedom of establishment and freedom to provide services"[6] less attractive. The subsequent 2010 Digital Agenda for Europe[7] largely carried over the objectives of the 1999 Communication "An information society for all"[8]. In summary, the regulatory orientation is characterised by a "*deregulatory approach*", where the main regulatory objective was to "*liberalise the internet*" and to bring the digital transition to the citizens mainly by removing burdens of digital services.[9] The prevailing regulatory tools include private-sector self-regulation and a general promotion of "flexible regulatory approaches"[10].

The second phase is linked to the 2015 Digital Single Market Strategy[11] and the legislation published in its context, whereas the GDPR can also be attributed to this phase. It is characterised by increased efforts to *balance de-regulatory goals with re-*

[1] See Savin, 'New directions in EU digital regulation post-2015: Regulating disruption' (2020) 11 *Pravni zapisi* pp. 93–120.

[2] Directive 2000/31/EC (OJ L 178, 17.7.2000, pp. 1–16).

[3] The principle of limited liability ensures that providers of "intermediary services" are except from liability for illegal content posted by their users. However, this exemption applies as long as the provider has no knowledge of the illegal activity and acts expeditiously to remove the illegal content, once notified. It therefore essentially consists of an avoidance of general monitoring.

[4] The country-of-origin principle dictates that online service providers are subject to the supervision by national authorities of the country where they are established, rather than of each country where their services are accessed.

[5] Directive 2006/123/EC (OJ L 376, 27.12.2006, pp. 36–68).

[6] Art. 5, Directive 2000/31/EC.

[7] COM(2010)0245 f/2.

[8] COM(1999)687.

[9] Interview with official at the European Commission.

[10] See Eberlein and Newman, 'Escaping the International Governance Dilemma? Incorporated Transgovernmental Networks in the European Union' (2008) 21 *Governance* pp.25–52.

[11] COM(2015) 192 final (SWD(2015)100). However, some interviewees of the EU Commission question the extent to which the Digital Single Market Strategy is a strategy that brings something new comparable to the first and third phases.

University of Vienna Law Review, Vol. 9 No 3 (2025), pp. 140-168, https://doi.org/10.25365/vlr-2025-9-3-140.

regulatory goals.[12] The strategy updates the 2010 goals to boost innovation and competitiveness through effective light-touch regulation. At the same time, its related Communications on platform economies[13] provide, for the first time, a critical analysis of monopolies created by the "winner takes it all mechanisms" of large online platforms.[14] A general awareness of the power of the "platform economy" is thus beginning to emerge, which is closely linked to the growing power of "data economy" and the resulting societal concerns about, for example, citizens' right to privacy online. Prominent laws that have been passed in this context are: the 2019 Platform to Business Regulation[15] addressing the principle of fairness for business-to-business relations; the 2019 Copyright Directive[16] introducing a new interpretation of the principle of liability; the 2021 Regulation on Terrorist Content Online[17] stressing the platform's responsibility in their content distribution by introducing monitoring obligations; and the GDPR[18], the most globally influential and powerful manifestation of a data governance framework.[19] In summary, the second phase adds to the regulatory goal of innovation and competitiveness, goals to ensure data control, privacy, safety, transparency and fairness. It can be noted that tensions occur between the goal of innovation and the goal of protecting individual fundamental rights, e.g. manifested in the GDPR. The regulatory tools are defined by an expansion of sector-specific regulation, a continued promotion of flexible regulatory instruments, characterised by a push for "agencification"[20] and an increase of non-binding

[12] See Laurent, *European Objects: The Troubled Dreams of Harmonization* (2022).

[13] COM/2016/0288 final, COM/2016/0320 final.

[14] Interview with official at the European Commission.

[15] Commission Regulation (EU) 2019/1150 (OJ L 186, 11.7.2019, pp. 57–79).

[16] Commission Directive (EU) 2019/790 (OJ L 130, 17.5.2019, pp. 92–125).

[17] COM(2018) 640 (OJ L 172, 17.05.2021, pp. 79-109).

[18] Regulation (EU) 2016/679 (OJ L 119, 4.5.2016, pp. 1–88).

[19] See Bradford, *The Brussels effect: how the European Union rules the world* , First issued as an Oxford University Press paperback ed. (Oxford University Press, 2021) p. 132. It should be noted that the majority of the GDPR's requirements were already reflected in the 1995 Data Protection Directive (Directive 95/46/EC OJL 281 , 23.11.1995 pp. 0031 - 0050). However, the latter was marked by poor enforcement and compliance and a low territorial reach. Moreover, the former additionally added two new obligations: the "right to be forgotten" and the "privacy by design" principle.

[20] Wallace, Pollack, Roederer-Rynning, Young (eds.), *Policy-Making in the European Union* , Eighth Edition ed. (Oxford University Press, 2020) 291.

guidelines and recommendations[21], besides a strong fundamental rights approach is introduced by the GDPR.

The third phase begins with the von der Leyen Commission agenda: the digital strategy "Europe fit for the Digital Age"[22] and the resulting policy programme "EU Digital Decade"[23]. The agenda differs from the previous phases in three main ways: 1. It aims for "*interrelatedness with sustainability goals*". 2. It focuses on "*digital sovereignty*" with the aim of creating a "*strategic autonomy*" for Europe – not only for reasons of competition[24], but also for geopolitical and security reasons.[25] 3. There is a new emphasis on "*European common digital goods*" and the protection of "*core European values*". All of these objectives can be found, for example, in the EU Data Strategy[26], and the related EU Data Governance Act[27], which i.a. seek to increase trust in data sharing to create "common European public data spaces"[28]. This strong *top-down, transition-driven agenda* is combined with a new wave of regulation, described by a high-level official of the EU Commission as "a new way of doing politics" or "the

[21] The most prominent examples are the 'EU Code of conduct on countering illegal hate speech online' (*European Commission*) <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#relatedlinks> accessed 20 March 2024; and the 'Memorandum of understanding on the sale of counterfeit goods on the internet' (*European Commission*) https://single-market-economy.ec.europa.eu/industry/strategy/intellectual-property/enforcement-intellectual-property-rights/memorandum-understanding-sale-counterfeit-goods-internet_en> accessed 20 March 2024.

[22] 'A Europe fit for the digital age Empowering people with a new generation of technologies' (*European Commission*) <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_en> accessed 15 August 2023.

[23] 'Europe's Digital Decade: digital targets for 2030' (*European Commission)* <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en> accessed 15 August 2023.

[24] There is an increasing focus on the fact that the next generation of economic growth will be generated by the data economy, this time however not from personal data, but from industrial data. It is therefore emphasised that in order to turn Europe into a serious global player, policies and investments must be made in the areas of data spaces, artificial intelligence, the Internet of Things, virtual worlds, etc.

[25] Especially due to COVID-19, the Russian war in Ukraine and the energy crisis, issues of vulnerabilities, supply chain dependencies and threat scenarios through cyberattacks have reinforced this narrative of "Europe fit for Digital Age" (Interview with official from the EU Commission).

[26] See 'The European Data Strategy' (*European Commission Factsheet*, 19 February 2020) <https://ec.europa.eu/commission/presscorner/detail/en/fs_20_283> accessed 22 August 2023.

[27] Regulation (EU) 2022/868 (OJ L 152, 3.6.2022, pp. 1–44).

[28] The European Data Strategy lists 9 common European data spaces, such as the "Common European health data space" (EHDS), whose sector-specific regulation is currently under negotiation.

kairos for the transition in EU policymaking"[29]. Among the most important legal frameworks is the Digital Services Package adopted in 2022, consisting of the Digital Services Act (DSA)[30] and the Digital Markets Act (DMA)[31]. While the former can be described as a rewrite of the E-Commerce Directive, the latter focuses on fair competition through *ex-ante rules* instead of the traditional ex-post antitrust interventions to regulate large platforms acting as "gatekeepers" – a regulatory approach that can be seen as a revolution in EU competition law. In addition the Artificial Intelligence Act[32] will be the first horizontal legislation in the EU to regulate AI systems, and in general the world's first comprehensive AI law.

This new regulatory wave has to deal with challenges that neither the national nor the European level has dealt with so far.[33] The legislative frameworks designed here are therefore experimental attempts to find solutions to different, steadily increasing problems. Broadly speaking, the regulatory goal of enhancing innovation and competitiveness is being joined by the goal of ensuring the protection of fundamental rights – with a number of new rights added, such as the right to human dignity and non-discrimination – and the goal of preventing collective and societal harm. In the era of big data, hyper-connectivity and AI, principles such as data control- and minimisation are, to a certain extent, being replaced by regulatory approaches that are more organised according to risk and safety.

It is particularly interesting to see how attempts are being made to combine the different goals in the regulatory frameworks and, above all, how the new challenges of societal harm are being addressed. Although there is a clear increase of horizontal regulations, a first look at the promoted regulatory instruments of the third phase suggests that they do not differ fundamentally from the first phase, as they are, to a certain degree, based as well on classical EU internal market law.[34] This can be seen,

[29] Interview with official at the European Commission.

[30] Regulation (EU) 2022/2065 (OJ L 277, 27.10.2022, pp. 1–102).

[31] Regulation (EU) 2022/1925 (OJ L 265, 12.10.2022, pp. 1–66).

[32] '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 - Analysis of the final compromise text with a view to agreement' (*Council of the European Union,* 26 January 2024) <https://data.consilium.europa.eu/doc/document/ST-5662-2024-INIT/en/pdf> accessed 20 March 2024 – the analysis in this text will refer in most cases to this final compromise text of the AI Act proposal, adopted by the EU Parliament on 13 March 2024. If it refers to the Commission 2021 proposal (COM/2021/206 final (2021/0106 (COD) (2021), it will be indicated.

[33] Interview with official at the European Commission.

[34] Interview with CEPS thinktank researcher Perarnaud (Interview 5).

University of Vienna Law Review, Vol. 9 No 3 (2025), pp. 140-168, https://doi.org/10.25365/vlr-2025-9-3-140.

for instance, in a closer examination of the draft AI Act and the DSA. In the following, the AI Act will be discussed first and then the DSA, as the AI Act stands out in terms of its tensions and regulatory challenges.

III. Regulation of Artificial Intelligence – The AI Act

The AI Act represents one of the most complex and eclectic legal frameworks in the EU'swave of digital regulation. As it is explained in the respective recital, it is characterised by the aim to balance and combine diverging regulatory goals: First, the regulation has the objective to stimulate investment and innovation by facilitating the development of the internal market and preventing market fragmentation.[35] In this sense, the proposal is introduced by an emphasis on the EU's aspiration to be a global player in the development of new technologies. This goal to increase the European economy's competitiveness on the global market can best be understood by reading the proposal in the context of the EU's AI strategy[36]: a "geopolitical strategy"[37], consisting of the objective to build an "eco-system of excellence" (the promotion of AI-driven innovation through industry- and research funding), which – as it is explained – can only be unleashed by simultaneously building an "ecosystem of trust" (regulatory mechanisms to ensure "trustworthy AI"). Second, an essential component of the AI Act is to ensure the protection of fundamental rights, linked to the various rights in the Charter of Fundamental Rights (Charter), such as the right to human dignity, non-discrimination, data protection, the rights of the child, freedom of assembly etc. Third, the proposal aims to guarantee a protection of people in the Union from AI systems that cause further material or immaterial harms 1.) to individuals (e.g. AI systems restricting a person's freedom of choice by subliminal manipulative techniques, potentially causing thereby psychological harms), 2.) to social groups (e.g. AI systems providing social scoring), and 3.) to the general public interest (e.g. AI systems for 'real-time' remote biometric identification of natural persons, evoking a feeling of constant surveillance in a society).

---

[35] It is stressed in the Explanatory Memorandum of the Artificial Intelligence Act 2021 European Commission Proposal that the proposal presents an "approach to AI that is limited to the minimum necessary requirements to address the risks and problems linked to AI, without unduly constraining or hindering technological development or otherwise disproportionately increasing the cost of placing AI solutions on the market." (COM/2021/206 final, 3).

[36] COM (2020) 65 final, 2020, available here: (*European Commission*) <https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en accessed> accessed 15 August 2023.

[37] Interview with Dunlop, European Public Policy Lead at the Ada Lovelace Institute (Interview 11).

The AI Act's aim of creating a balance between these diverging regulatory goals can already be seen if one takes a first look at the structure of the legal framework: the regulatory system is a "patchwork of different regulatory regimes"[38], which is centred on a *risk-based regulatory approach*. It distinguishes four levels of risk, to which AI systems can be assigned: unacceptable risks, high-risks, limited risks and minimal risks. In addition, the final version of the AI Act introduces requirements for "General Purpose AI Models". The two latter categories (Title IV & Title V) contain i.a. (minimal) transparency requirements[39] and apply to approximately 80% of the AI systems circulating in the EU.[40] At the top of the pyramid of risks are AI applications that are considered a "threat to EU values".

A. General Purpose AI (GPAI)

Following the release of GPT-3 and -4 by Open AI, new provisions have been introduced to regulate "General Purpose AI Models" (GPAI) – based on a two-tier system (Title VIIIA): All GPAI model providers are subject to certain obligations such as complying with the Copyright Directive and publishing a summary about the content used for training. In addition, providers of GPAI models with *systemic risks* (their training involves a significant amount of computational power and has therefore "high-impact capabilities"[41]) are required to i.a. assess and mitigate potential systemic risks[42], to track and report serious incidents and to ensure adequate cybersecurity

[38] Interview with a stakeholder.

[39] Limited risks include deep fakes and chatbots. Minimal risks, which are unregulated, refer to spam filters or AI-enabled video games.

[40] Interview with Hakobyan, Advocacy Advisor on AI Regulation at Amnesty International (Interview 12).

[41] It is basically about how large the model is, and therefore how influential it is. In addition to the providers, the Commission is also empowered to designate a GPAI model as a systemic risk model if it meets the applicable threshold for high-impact capabilities. The concrete thresholds, as well as the tools and benchmarks for assessing high-impact capabilities are set and adjusted over time by the AI Office through a multi-stakeholder consultation process. (Recital 60n Artificial Intelligence Act final compromise text). The designation process is thus, to a certain extent, comparable to that for VLOPs and VLOSEs in the DSA and is likely to involve similar challenges (in terms of disputes over whether the designation was justified, etc.). It seems that so far only two models, namely OpenAI's GPT-4 and likely Google DeepMind's Gemini will be classified as GPAI with systemic risks ('Artificial Intelligence – Questions and Answers' (*European Commission*, 1 August 2024) <https://ec.europa.eu/commission/presscorner/detail/en/qanda_21_1683 > accessed 13 March 2024).

[42] "Systemic risks" include a range of risks beyond, for example, the list of systemic risks in the DSA - from which this approach is inspired - such as: chemical, biological, radiological, and nuclear risks; the capacity to control physical systems and interfere with critical infrastructure, risks from models of making copies of themselves or "self-replicating" or training other models; risk that a particular event

University of Vienna Law Review, Vol. 9 No 3 (2025), pp. 140-168, https://doi.org/10.25365/vlr-2025-9-3-140.

protection.[43] Compliance to these obligations can be demonstrated through "codes of practice"[44] until European harmonised standards are published. They provide guidance, for example, on how to identify the nature and type of systemic risk and how to mitigate it.[45]

B. Prohibited AI Practices

The final text of the Act outlines the following prohibited practices (Title II): - *AI systems deploying subliminal, manipulative, or deceptive techniques; - AI used to exploit the vulnerabilities of people (due to their age, disability, social or economic situation); - biometric categorisation systems that use sensitive characteristics (e.g. political, religious, philosophical beliefs, sexual orientation, race, with exemptions for law enforcement); - social scoring; -real time biometric identification in public accessible spaces for law enforcement (with exceptions); predictive policing solely based on profiling or personality traits; unauthorised facial recognition databases; emotion recognition systems in the areas of workplace and education institutions.*[46]

C. High-Risk AI Systems

The category of high-risk AI systems (Title III) builds the core of the legislation, referring to applications of AI systems that pose high-risks to public interests as regards "health, safety and fundamental rights"[47], which are nonetheless deemed manageable. It covers so called "stand-alone AI systems" in a wide range of areas, mainly deployed in the public sector, and lists in the final version: - *non-banned biometrics (remote biometric identification systems, emotion recognition systems etc.); - critical infrastructure (management of road traffic, electricity etc.); - education*

---

could lead to a chain reaction with considerable negative effects that could affect up to an entire city, an entire domain activity or an entire community; etc. (Recital 60m Artificial Intelligence Act final compromise text).

[43] Art 52d, Artificial Intelligence Act final compromise text (Title VIIIA).

[44] Art 52e, Artificial Intelligence Act final compromise text (Title VIIIA).

[45] A provider of a GPAI models can be subject to potential fines of up to 3% of its total worldwide turnover in the preceding financial year or 15 million EUR, whichever is higher (Art 72a, Artificial Intelligence Act final compromise text (Title X)). The EU Commission will be solely competent for the supervision and enforcement.

[46] Art 5, Artificial Intelligence Act final compromise text (Title II). The final compromise text allows for fines up to 35 million EUR or 7 % of the total worldwide annual turnover of the preceding financial year (whichever is higher) for violations involving prohibited practices (Art 71, Artificial Intelligence Act final compromise text (Title X)).

[47] Recital 4aa, Artificial Intelligence Act final compromise text.

(AI systems determining access to educational institutions, evaluating learning outcomes etc.); - employment and workers management (AI systems used for recruitment, evaluation of job performance, allocating tasks etc.); - access to essential public services and benefits (AI systems assessing eligibility to benefits and services, risks assessments in health insurance, evaluation of creditworthiness etc.); - law enforcement (polygraphs, predictive policing not solely based on profiling or personality traits etc.); - migration, asylum and border control management (examination of asylum complaints, assessment of irregular migration etc.); - administration of justice and democratic processes (AI systems that research facts and apply the law to them, influence election results or voting behaviour).[48]

In addition, it includes AI systems that are intended to be used as safety component of products, which are already subject to third party conformity assessment.[49] The ex-ante classification of high-risks can be updated by *delegated acts*, for the adoption of which the Commission is empowered.[50]

D. Regulatory Instruments of High-Risk AI Systems

1. Filter Provision

In the final version of the proposal, a substantial amendment has been introduced which stipulates that AI systems falling into the above categories do not necessarily have to be classified as high-risk in the following circumstances: if they intend - to *perform a narrow procedural* or *preparatory task*, - to *improve previously completed human activity* or *assessment*. If, however, an AI system performs profiling of natural persons (e.g. automated processing of personal data to assess job performance), it shall always be considered as high-risk. Providers who consider that their AI system does not fall within the high-risk classifications need to document their assessment before placing the system on the market or putting it into service and make the documentation of the assessment available to the competent national authorities *upon request*.[51] This addition, which allows providers to decide on the basis of a *self-assessment* whether their AI system is not high-risk and to place it on the market without having to comply with the rules for high-risk systems if the assessment is in

[48] Artificial Intelligence Act final compromise text, Annex III.

[49] Art 6, Artificial Intelligence Act final compromise text (Title III).

[50] Art 7, Artificial Intelligence Act final compromise text (Title III).

[51] Art 6 2a-2b, Artificial Intelligence Act final compromise text (Title III).

University of Vienna Law Review, Vol. 9 No 3 (2025), pp. 140-168, https://doi.org/10.25365/vlr-2025-9-3-140.

their favour, is more business-friendly compared to the Commission's AI Act proposal.[52]

2. Fundamental Rights Impact Assessment

Moreover, the final AI Act version introduced a requirement for deployers acting in the context of public service provision to perform a *fundamental rights impact assessment*, to evaluate the potential negative effects that the use of a system may have on fundamental rights. It includes descriptions of the categories of natural persons and groups likely to be affected by its use, the specific risks of harm, and the measures to be taken in the event of those risks materialising, such as internal control mechanisms. The deployer shall notify the market surveillance authority of the results of the assessment.[53] How exactly these impact assessments will be carried out and whether technical standards will be developed by European standardisation bodies (ESOs) together with the AI Office is still an open and highly controversial issue that concerns both civil society and the ESOs themselves.[54]

3. Standard-setting process

The legal framework of Title III is based on the New Legislative Framework (NLF)[55], which sets out a general structure for *EU product legislation*. Its main aim is the enlargement and smooth functioning of the internal market for industry, by ensuring that products are safe so that they can benefit from the principle of *free movement of goods*. This "*product safety regime*" has the following characteristics: 1. It consists of a combination of a set of "essential requirements" (secondary EU law) that products must meet to circulate freely within the EU market. 2. Such legally binding obligations are combined with voluntary, harmonised technical standards, developed by ESOs, which are independent from the EU institutions. These are composed of national delegations, characterised by an over-representation of industry interests and a very low level of participation by civil society groups, due to a lack of resources.[56] Although the participation of civil society interest groups is promoted at the EU level

[52] Interview with Uuk, EU Research Lead at the Future of Life Institute (Interview 14).

[53] Art 29a Artificial Intelligence Act final compromise text (Title III).

[54] Interview with Uuk, EU Research Lead at the Future of Life Institute (Interview 14).

[55] The NLF was adopted in 2008 to provide a revision of the "new approach to harmonisation", which came to prominence in the 1980s and was designed as a new approach within the Single Market programme to allow greater flexibility in product harmonisation legislation.

[56] See Craig and De Búrca, *EU law: text, cases, and materials* , Seventh edition ed. (Oxford University Press, 2020) 167.

University of Vienna Law Review, Vol. 9 No 3 (2025), pp. 140-168, https://doi.org/10.25365/vlr-2025-9-3-140.

through financial subsidies by the Commission, the voices of civil society are sidelined when decisions are made by voting, where only national delegations can participate. 3. Manufacturers can choose to either meet the essential requirements on their own way or to apply the harmonised European standards. Usually, there is an incentive for the latter, due to a presumption of conformity in cases of compliance, which automatically grants access to the internal market. 4. The conformity assessment and "CE marking" is normally undertaken by the manufacturers of the products themselves, in some cases however, conformity assessment bodies ("notified bodies") assess whether the products confirm with the product safety requirements.

A criticism of this regulatory regime – when having the industrial economy, which it was developed for, in mind – is hence among others the low consumer participation at national level and the insufficient decision-making powers for civil society interest groups at EU level. In addition, the requirements for conformity assessment, which usually rely on the responsibility of industry, are commonly criticised.[57]

It can be noted that the transfer of the product safety regime to the digital economy poses additional challenges for standards setting activity as well as for EU legislation in general that did not exist before.[58] On the one hand, the approach is in line with the EU's better regulation guidelines, since it is considered as a light regulatory approach. In this sense, a core objective of regulation can be fulfilled: namely the flourishment of the single market for AI, as a result of "higher demand due to higher trust, more available offers due to legal certainty, and the absence of obstacles to cross-border movement of AI systems"[59]. On the other hand, some civil society organisations, consumer representatives and experts have expressed doubts, as the decision to base the regulation on the product safety model clearly influences how AI is defined, what is considered as "trustworthy and ethical AI", which actors are accountable in the decision-making and oversight, and which actors are considered liable in the event of potential harm.

---

[57] See Micklitz, 'The Role of Standards in Future EU Digital Policy Legislation - A Consumer Perspective' (2023) *Commissioned by ANEC and BEUC*. See Veale and Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act — Analysing the good, the bad, and the unclear elements of the proposed approach' (2021) 22 *Computer Law Review International* pp. 97–112.

[58] These fundamentally new challenges to EU legislation were highlighted by several senior officials in the interviews.

[59] Explanatory Memorandum of the Artificial Intelligence Act 2021 European Commission Proposal 10.

A consequence of this regulatory approach is that AI is consistently defined as a *product* whose aim is to circulate freely in the internal market. It follows that a wide range of high-risk AI systems are authorised to gain access to the EU market, *if* they abide to a set of requirements. These requirements consist of more general obligations for: - *quality and risk management systems*, - *high-quality training data-sets, - record-keeping, - instructions for use to deployers, - human oversight*, - *transparency, - accuracy, - robustness and - cybersecurity* of AI systems.[60] In addition, there is an obligation for standalone high-risk AI systems to be registered in an EU Commission database.[61] A precise specification of these general requirements takes place on the basis of the elaboration of certifiable harmonised, technical standards by the ESOs (CEN, CENELEC).[62] As a result, M. Veale and F. Borgesuis argue: "standardisation is arguably where the real rule-making in the draft AI Act will occur"[63]. In order to determine whether a (stand-alone) high-risk AI system is compliant with the standards, the providers[64] are in most cases then free to undergo a self-assessment[65]. In some cases a third-party conformity assessment by notified bodies is required (e.g. remote biometric identification).[66]

It can be noted that the focus here is on how to ensure that an AI system is "*ethical-by-design*"[67] – how to verify whether a given AI system is biased, how to increase its robustness, etc. – and less on the *context of use*. This is because the logic of the product safety model, assumes that a product is safe if it meets certain *technical requirements*. However, some experts and stakeholders point out that comparing an AI system to a product such as a toy is challenging, as the deployment of AI in public

[60] Arts 9–15, Artificial Intelligence Act final compromise text (Title III).

[61] Art 60, Artificial Intelligence Act final compromise text (Title VII).

[62] The Commission recently called for 10 mandated standards. See: COM(2023) 3215 final, 22.05.2023.

[63] Veale and Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act — Analysing the good, the bad, and the unclear elements of the proposed approach', 105.

[64] The "providers" are, in the logic of the product safety regime, the developers or "manufacturers" of the AI technology, who sell it in the Union market, whereas the "deployers" or "users" are those who deploy the system – for instance a municipality.

[65] Points 2-8 of Annex III, Artificial Intelligence Act final compromise text.

[66] Point 1 of Annex III, Artificial Intelligence Act final compromise text.

[67] Smuha, 'The Human Condition in An Algorithmized World: A Critique through the Lens of 20th-Century Jewish Thinkers and the Concepts of Rationality, Alterity and History, SSRN (December 2021), 1, http://dx.doi.org/10.2139/ssrn.4093683

University of Vienna Law Review, Vol. 9 No 3 (2025), pp. 140-168, https://doi.org/10.25365/vlr-2025-9-3-140.

sectors such as for law enforcement, for the assessment of legitimacy for public benefits, for border control etc. could pose risks (some as yet unknown) that affect the public interest and, unlike a classical product, is very likely to lead to fundamental societal transformations. This shift of the product safety regime away from the *use* of an AI system has the potential to create a premature or false impression of safety. One interview partner explains hereto:

"This approach proposes the idea that as long as you can mitigate some technical risks, then the problems are solved...as long as you place some kind of technical means of debiasing, human oversight measures etc. into the system, then everything seems fine. But we should be more critical about what kind of systems we actually accept as maybe a society to be used."[68]

There is therefore a probability that if a system falls into a high-risk category, and if it confirms to the standards, its use becomes automatically legitimised. This legal approach could hence lead to a general *legitimisation* and *normalisation* of the use of AI systems in these high-risk categories – a development that is certainly supported by the regulation, as it says in the introduction: it is "preventing Member States from imposing restrictions on the development, marketing and use of AI systems, unless explicitly authorised by this Regulation"[69].

Another consequence of the focus on *bringing ethical values in the product design* of the AI system, so that it can flow as a safe product in the single market, is that the main duties lie with the providers, who - like any manufacturer placing a product on the EU market – are also liable for damage caused by their defective products.[70]

What concerns the standard setting process, the main challenge of the transfer of the classic product safety legislation to the digital environment consists of the fact that the ESOs are dealing here with "*socio-technical standards*"[71]. For example, in a standard-

[68] Interview with Hakobyan, Advocacy Advisor on AI Regulation at Amnesty International (Interview 12). Another interview partner mentioned: "*It's true that if the institutions say: Okay, we are going to allow this.. then it goes to the standard-setting bodies and it becomes something that is operationalised by standards.. then it is true that that gives the idea that it must be safe to do it.*" Interview with Dunlop, European Public Policy Lead at the Ada Lovelace Institute (Interview 11).

[69] Recital 1, Artificial Intelligence Act Proposal.

[70] Obligations for deployers are primarily formulated in Title IV, in the context of *transparency requirements for limited risk AI systems*. For example, if a user posts a deepfake video, they must label it as such, or if a person interacts with a chat bot on a website, the provider must inform them that it is not a real person.

[71] Micklitz, 'The Role of Standards in Future EU Digital Policy Legislation - A Consumer Perspective' (2023) *Commissioned by ANEC and BEUC,* 19.

University of Vienna Law Review, Vol. 9 No 3 (2025), pp. 140-168, https://doi.org/10.25365/vlr-2025-9-3-140.

setting process for refrigerators, it is not difficult to develop a standard for measuring the temperature of refrigerators so that every fridge is measuring the same temperature. In the case of the AI Act, standard-setting bodies now face the challenge of developing standards for AI systems that shall prevent, for instance, discrimination. Hence, they have a clear mandate to integrate fundamental rights, however, the regulatory design lacks guidance on how to do that.[72] In contrast to standards for measuring the temperature of refrigerators, the aim here is to develop standards by means of which it will be technically possible to measure the extent to which an AI system violates fundamental human rights, such as the right to non-discrimination, human dignity, etc., thereby touching upon legal, as well as normative, ethical, and even political questions, for which, however, standard setting bodies are ill-equipped.[73] This means, that even the technical level, where "the real rule-making" is shifted to, is strongly interwoven with public interests.[74] – These challenges are, to a certain extent, increasing with regard to fundamental rights impact assessments, filter provisions and GPAI risk assessments.

As far as conformity assessments for high-risk systems, but also fundamental rights impact assessments, self-assessments in the context of filter provisions and GPAI risk assessments are concerned, there is the additional challenge for deployers and users to evaluate whether their systems are compliant with – in most cases – socio-technical standards. For this, no usual technical checklists can be applied, instead complex, interdisciplinary assessments must be carried out that require the necessary *expertise*. It also requires the establishment of competent oversight mechanisms.

E. How to Address the Challenges of (Self-) Assessment Processes and Technical, Private-Sector Standard Setting?

In order to address the lack of accountability and liability arising from the power of market interests in the various assessment procedures and standard-setting processes, which has been exacerbated by the transfer of the NLF to the digital environment, consumer representatives advocate voting rights for consumer, civil society and

[72] See Micklitz, 'The Role of Standards in Future EU Digital Policy Legislation - A Consumer Perspective' (2023) *Commissioned by ANEC and BEUC,* 24.

[73] Interview with a stakeholder.

[74] For instance, an AI system used in the education sector – therefore it is high-risk – to determine access to a specific educational training bears the risk, as it is stated in the regulation, to violate *the right to education and training* as well as *the right to non-discrimination*. It must therefore be guaranteed by standards that the AI design does not allow such violations of human rights. These standards are based on normative, value-laden evaluations which, in the best case, are oriented towards concrete *use case studies*. Consequently, there is no "objectively correct" answer or decision to make.

University of Vienna Law Review, Vol. 9 No 3 (2025), pp. 140-168, https://doi.org/10.25365/vlr-2025-9-3-140.

independent experts in standard-setting bodies at EU level, with the aim of centralising the standard-setting process. To counteract the "privatisation of standard making process", they argue moreover that harmonised standards should become legal norms, thus losing their voluntary nature, which has left much room for industry to manoeuvre.[75] With regards to the entire AI Act, thinktanks such as the Ada Lovelace Institute additionally highlight the importance of multistakeholder participation for public oversight. To allow for a balanced and strong "ecosystem of inspection" or an "ecosystem of audits", it is argued that the "AI Board" as well as the "AI Office" at EU level should have an essential function with sufficient competences.[76] The final version of the AI Act could meet these demands to a certain extent: The "AI Office"[77] – a new, more centralised body at the Commission primarily responsible for monitoring and enforcing GPAI models[78] – aims to establish a stronger link with the scientific community by collaborating with the "Scientific Panel"[79] – an advisory body to the AI Office and national competent authorities, composed of independent scientific experts, to be established by the Commission through an implementing act. The "AI Board"[80], on the other hand, will be composed of designated representatives of the Member States and will be attributed with an advisory function to the Commission, national competent authorities and the AI Office. However, the extent to which these new governance structures at EU level can function as "participatory oversight bodies" remains open.

In summary, civil society and independent experts emphasise the significance of rigorous participation mechanisms at various levels, practices, and institutions. These mechanisms ought to encompass *fundamental rights impact assessments, assessments concerning high-risk classifications, risk assessments related to systemic risks of GPAI models, standard-setting bodies, conformity assessments, AI Board, AI Office, and national competent authorities*. This is emphasised to be an important measure to guarantee that the AI Act becomes "a living piece of legislation", to align

[75] Interview with a stakeholder.

[76] Interview with Dunlop, European Public Policy Lead at the Ada Lovelace Institute (Interview 11).

[77] Chapter 3, Artificial Intelligence Act final compromise text (Title VIIIA).

[78] The AI Office is, for instance, responsible for the drawing up, review and adaption of Codes of Practice for GPAI Models.

[79] Art 58b, Artificial Intelligence Act final compromise text (Title VI).

[80] Art 58, Artificial Intelligence Act final compromise text (Title VI).

AI with public values, to ensure that AI is used for the public good and that human rights are adequately protected.[81]

IV. The Regulation of Digital Services – The DSA

Similarly to the AI Act, the Digital Services Act (DSA) seeks to strike a balance between different regulatory goals, which are partly difficult to reconcile: First, it aims to facilitate innovation by striving for the harmonisation of rules for information society services "for a safe, predictable and trusted online environment"[82] without significantly interfering with the business models of online platform services. The regulation can be seen as a cautious update of the E-Commerce Directive, maintaining its core principles for stimulating innovation. Second, the regulation provides several harmonised due diligence obligations for online platforms (such as social media platforms, online marketplaces, information retrieval encyclopaedias, search engines) to tackle potential infringements of a long list of fundamental rights enshrined in the Charter. Third, the due diligence obligations also relate to dark patterns and further systemic risks, stemming from the design or functioning of platform services, which include foreseeable collective, broad societal harms in the Union.

As the legal framework is a continuation of the E-Commerce Directive, its regulatory instruments differ from the AI Act's product regulation approach mainly in that the focus does not lie on a specific system (e.g. AI system), but on the companies that have to fulfil certain due diligence obligations - independent of the type of AI applications. The regulatory approach here is characterised by a strong combined with stronger centralised supervisory powers of the Commission.

A. Online Platforms

In general, the DSA can be conceptually divided into obligations that apply to all platforms[83] and those that apply only to very large online platforms (VLOPs) and search engines (VLOSEs)[84]. As regards the former, the DSA formulates stricter rules

[81] Hertie Futures Forum (Berlin, 06 March 2024): 'Too smart to regulate? How Al challenges good governance'. Henrik Enderlein Forum, Hertie School.

[82] Recital 109, Digital Services Act.

[83] This includes online platforms (e.g. online market places), hosting services (e.g. cloud hosting services), intermediary services (e.g. internet access providers).

[84] VLOPs and VLOSEs are classified by the DSA as platforms or search engines that have more than 45 million users per month in the EU, that is, a number equivalent to 10 % of the Union population.

University of Vienna Law Review, Vol. 9 No 3 (2025), pp. 140-168, https://doi.org/10.25365/vlr-2025-9-3-140.

for content moderation to monitor illegal content online, requiring i.a. that appropriate "notice and action mechanisms" are in place that follow the concept of "what is illegal offline should be illegal online"[85]. Moreover, targeted advertising based on profiling by sensitive personal data such as ethnicity, political views or sexual orientation is prohibited[86], measurements for online protection of minors are introduced[87], and general transparency requirements regarding online advertisements and recommender systems are established[88]. In addition, "dark patterns" are prohibited, meaning practices which aim, via the online interface design and organisation, to nudge and manipulate users of a service, thereby restricting their autonomy and freedom of choice.[89]

B. Very Large Online Platforms

What concerns obligations that apply only to VLOPs and VLOSEs, they could be seen as the crucial and most debated part of the regulation. As it is explained in the recitals:

"*Given the importance of very large online platforms, due to their reach (...) in facilitating public debate, economic transactions and the dissemination to the public of information, opinions and ideas and in influencing how recipients obtain and communicate information online, it is necessary to impose specific obligations on the providers of those platforms.*"[90]

It is stressed further that these platforms bear the danger of causing "societal risks" since "the way they design their services is generally optimised to benefit their often

---

The designation process is run by the Commission, which has currently designated the following VLOPs and VLOSEs: AliExpress, Amazon (Amazon Store), Apple (App Store), Aylo Freesites Ltd. (Pornhub), Booking.com, Google (Google Search, Google Play, Google Maps, Google Shopping, Youtube), LinkedIn, Meta (Facebook, Instagram), Microsoft (Bing), Pinterest, Snap (Snapchat), Technius (Stripchat), TikTok, Twitter (X), WebGroup (XVideos), Wikemedia Foundation Inc 3**** (Wikepedia), Zalando ('Supervision of the designated very large online platforms and search engines under DSA' (*European Commission,* information updated on 14 March 2024) <https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses> accessed 22 March 2024).

[85] See Recital 12, Digital Services Act.

[86] Art 26, Digital Services Act.

[87] Art 28, Digital Services Act.

[88] Art 27, Digital Services Act.

[89] Art 25, Digital Services Act; Recitals 67 Digital Services Act.

[90] Recital 75, Digital Services Act.

University of Vienna Law Review, Vol. 9 No 3 (2025), pp. 140-168, https://doi.org/10.25365/vlr-2025-9-3-140.

advertising-driven business models", which "can cause societal concerns". As they "can be used in a way that strongly influences safety online, the shaping of public opinion and discourse, as well as online trade" this could lead to fundamental "societal and economic harm".[91] These systemic risks stemming mainly from the *design and functioning of the services* include: 1.) *the dissemination of illegal content online* (e.g. illegal hate speech), 2.) *negative (foreseeable) impacts on the exercise of fundamental rights* (such as the right to freedom of expression and information, including media pluralism, to human dignity, to non-discrimination (e.g. occurring from discriminatory content moderation and profiling)), 3.) *negative (foreseeable) effects on civic discourse, democratic-, electoral processes and public security*, 4.) *(foreseeable) risks stemming i.a. from "coordinated disinformation campaigns"* (e.g. in relation to gender-based violence or the protection of public health).[92]

1. Regulatory Instruments of Very Large Online Platforms

To identify, analyse and address any of those risks it is required that very large online platforms conduct *risk assessments* (RAs) on an annual basis taking into account specifically the design of recommender systems, advertising systems, content moderation processes and other data related practices. RAs are a common method in EU consumer law, requiring companies to conduct assessments for a wide range of risks, but this is the first time that RAs will be carried out for online content and conduct to address "systemic risks" that arise in this context.[93] Where such *self-assessments* identify systemic risks, VLOPs and VLOSEs are required to take reasonable measures to *diligently mitigate* the risks, for example by adapting their recommender, content moderation or advertising systems.[94] These risk mitigation measures are hence *self-regulatory measures*, which might be however combined with *co-regulatory cooperation* with the EU Commission and/or other service providers, such as *codes of conduct*[95] or *industry best practices*. The legal framework therefore uses, through these self- and co-regulatory agreements, *voluntary non-harmonised industry standards*, in contrast to the AI Act's product safety regime.

[91] Recital 79, Digital Services Act.

[92] Article 34, Section 5, Digital Services Act.

[93] In particular, the systemic risk assessments of the GPAI models in the AI Act will follow this model.

[94] Art 35, Digital Services Act.

[95] As one interviewee points out, codes of conduct developed by the Commission through a co-regulatory process at EU level could have the potential to provide clear guidance to the platforms' systemic mitigation measures as well as to the risk assessments.

University of Vienna Law Review, Vol. 9 No 3 (2025), pp. 140-168, https://doi.org/10.25365/vlr-2025-9-3-140.

In order to ensure the verification of independent experts, the law provides that the risk assessment reports as well as the mitigation measures are, in a second step, subject to third-party *independent audits*, which are usually conducted by the big four largest consultancy firms. In addition, "vetted researchers" are required to get access by VLOPs and VLOSEs to data, in order to contribute to the detection, identification and understanding of systemic risks.[96] The audit reports are then transmitted together with the risk assessments and the mitigation measures to the Commission, the European Board of Digital Services ("the Board")[97], the Digital Service Coordinators ("DSC")[98] and the European Centre for Algorithmic Transparency ("ECAT")[99]. These institutions evaluate the reports and mitigation measures, possibly by requesting additional data from the platform or reaching out to independent experts and vetted researchers. It is then – similarly to the provision of GPAI models in the AI Act – ultimately up to the Commission to determine whether the online platform has infringed the obligations laid down by this regulation. In the most serious cases, it can directly impose fines up to 6% of the annual worldwide turnover of the service provider.[100] This gives the Commission supervisory powers it has never had before. For the first time, it will become a direct regulator of large companies, going beyond competition law.

As the risk assessments are not based on harmonised European standards, civil society interest groups in particular criticise – and tech companies admit – that it is not clear *how* and *what* is going to be assessed. This lack of clear guidance for VLOPs and VLOSEs leaves them hence with a lot of leeway to decide how to assess risks in order to comply with the DSA's due diligence obligations. This approach of the legal framework to provide an *overarching, flexible framework* for systemic risks is however also comprehensible, as it is noted in an interview by a data scientist and co-founder of the NGO "Algorithm Audit", since the notion of systemic risks can only be understood as a "complex, context-dependent concept".[101] Yet, it would need a

[96] Article 40, Digital Services Act. Researchers can access specific data from platforms by sending a data access request to the DSC. The DSC itself has been given this new data access capability to help monitor and mitigate systemic risk.

[97] "The Board" is – similarly to the "AI Board" – an advisory body and information system between the Commission and the member states, consisting of Commission officials and representatives from the national DSCs.

[98] The DSC is the authority identified by the member state to supervise and enforce the DSA.

[99] ECAT is a Centre of experts managed by DG CNCT and the JRC of the European Commission.

[100] Article 52, Digital Services Act.

[101] Interview with Parie, Director of Algorithm Audit (Interview 13).

University of Vienna Law Review, Vol. 9 No 3 (2025), pp. 140-168, https://doi.org/10.25365/vlr-2025-9-3-140.

specification on a case-based level to define what systemic risks are, in the context of social media, information retrieval encyclopaedias, online marketplaces etc. to better answer the big question "*What makes a risk systemic?*".[102]

In addition, similar challenges of those underlying the AI Act's standardisation processes as well as the AI assessment procedures can be identified: RAs need to measure i.a. macro-impacts of algorithmic systems on social groups or an entire society. This makes systemic risk assessments in the online space fundamentally different to classic assessments which are normally carried out as technical checklist routines, requiring mainly technical competences.

In the case that a VLOP, such as a social media platform, needs to evaluate a specific risk scenario such as "systemic risks to public health", the following questions need to be clarified, as explained by an expert of the thinktank "Stiftung Neue Verantwortung": Who is the affected party? (e.g. adults, children); What are the characteristics of the potential risk? (e.g. mental health problem); What specific harm does the group experience? (e.g. eating disorder); What elements of the platform might cause the risk? (e.g. specificities of the personalisation patterns of algorithms, promoting certain content); What are foreseeable macro-impacts on a society? (e.g. mental health crisis of young adults in the long run).[103] Moreover, it must be answered whether and which fundamental rights, enshrined in the Charter, are violated. The challenge, therefore, is to *operationalise abstract principles*, to measure macro-level socio-legal harms to social groups and the society as a whole. RAs hence need to be conducted on the basis of complex interdisciplinary ethical, legal, sociological, psychological and technical evaluations and complicated long-term impact assessments. In this context, the *normative dimensions* of the design of recommender system, such as the underlying normative methodological choices, also need to be considered and disclosed.[104] The assessment of systemic risks for online content and behaviour therefore requires extensive expertise.

Some civil society organisations are concerned in addition that VLOPs and VLOSEs would have little incentive to publish critical reports on their engagement-centred

[102] Interview with Parie, Director of Algorithm Audit (Interview 13).

[103] See Messmer, 'Afternoon Sessions - DSA Stakeholder Workshops' (*European Commission DG CNCT*, 27 June 2023) <https://ec.europa.eu/newsroom/dae/items/789062/en> accessed 15 August 2023.

[104] Algorithm Audit, *White paper – Feedback on DSA Delegated Regulation (conducting independent audits)* (2023). s. (*Algorithm Audit*) <https://algorithmaudit.eu/knowledge_base/white_paper_dsa_delegated_regulation_feedback/> accessed 15 August 2023.

University of Vienna Law Review, Vol. 9 No 3 (2025), pp. 140-168, https://doi.org/10.25365/vlr-2025-9-3-140.

design of their algorithms (which, for example, are based on normative choices that result in engagement-centric algorithms that spread polarising content or cause addictive behaviour), as this could threaten their business model.

These challenges also apply to independent third-party auditing and the development of appropriate mitigation measures. Traditionally, audits in the financial-, medical- or IT sector are conducted – similarly to RAs – as technical checklist routines. Private auditors therefore need acquire enormous expertise to audit specific AI systems. In contrast to previous audit procedures, auditing methodologies must be developed here that can also capture normative, ethical and socio-legal aspects. Auditors thus stress that the lack of guidance on the criteria to be used in the audit risks subjective audits and that there is a lack of expertise to develop such auditing methodologies.[105]

What concerns the mitigation measures, as the legislative framework relies on self- and co-regulation, tech companies have the responsibility to find the appropriate methods to ascertain and mitigate certain systemic risks.[106] It is hence up to the industry to develop context-sensitive approaches to tackle for instance algorithmic discrimination or harmful polarisation. Some civil society representatives warn that this could water down the potential to combat systemic risks such as societal harms, which would be a lost opportunity for digital regulatory governance.[107]

C. How to Address the Challenges of (Self-) Assessment Processes and Third-Party Auditing?

It can be summarised that his regulatory regime is based on a "*market controls markets approach*"[108], where the third-party auditors (usually the big four consulting services) assess the self-assessment reports and mitigation measures of large online platforms. However, these platforms have become significant public facilities due to their reach and functionality. Social media platforms, for example, have become integral to the contemporary public sphere[109], with the capacity to profoundly

[105] Interview with a Senior Consultant at KPMG (Interview 3).

[106] Note that these challenges will also arise from the similar approach of the AI Act to GPAI models.

[107] See 'Afternoon Sessions - DSA Stakeholder Workshops' (*European Commission DG CNCT*, 27 June 2023) <https://ec.europa.eu/newsroom/dae/items/789062/en> accessed 15 August 2023.

[108] Interview with Parie, Director of Algorithm Audit (Interview 13).

[109] See Staab and Thiel, 'Social Media and the Digital Structural Transformation of the Public Sphere' (2022) 39 *Theory, culture & society* pp. 129–43. They explain how the public sphere and the role of the citizen have been structurally transformed by the digital socio-economic transformation. See also

influence social value systems or the direction of political discourse. At the meta-level, the regulator then steps in, having the supervisory and executive power to hold the platforms accountable for their due diligence obligations. The regulator - in this case the Commission - thus has the function of a "*meta-oversight*" and therefore has, to a certain extent, a limited role. This room for manoeuvre that tech companies retain thereby is criticised by scholars such as R. Griffin, who argues that this approach consequently suggests that "corporations can legitimately control the online public sphere if they make minor operational reforms, and side-lines criticism of their business models and market structure."[110]

To address this deficit of accountability, some experts advocate to strengthen *public oversight mechanisms* arguing that since large online platforms play an important and hugely defining societal role – comparable to public services – they should not be assessed by third party auditors, where only at the meta-level, the regulator steps in to ensure due diligence. Instead, these key assessments should be done by public bodies, with a certain degree of *democratic legitimacy*, characterised for instance by institutionalised civil society participation, to guarantee a *system of checks and balances*.[111]

This new relevance for public oversight mechanisms is discussed and recognised on the part of the Commission as well, as emphasised by an official:

"*That's also quite a novelty that we expect to open up public oversight (...) if we open up also to auditors, third parties, researchers, civil society, all can help us to get some findings on the results on whether what the platforms are promising or proposing as mitigation measures works or doesn't work. (...) We have ears and eyes everywhere.*"[112]

Herman, 'Felix Stalder, The Digital Condition' (2020) *International journal of communication (Online)* 4707-.

[110] Griffin, 'Rethinking rights in social media governance: human rights, ideology and inequality' (2023) 2 *European law open* pp. 0–56 at 33. However, recent developments have shown that the Commission takes this role very seriously and that its power should not be underestimated: the Commission is continuously sending formal requests for information to VLOPs and VLOSEs to provide more information on the measures they have taken to comply with the obligations regarding access to data, recommendation systems, risk management related to civic discourse, the methodology underlying risk assessments, etc. On the basis of the assessment of their replies, the Commission may open formal investigations, as it has already done in three cases: against X (for suspected breaches in the fight against disinformation, etc.), Tiktok (for possible breaches in the protection of minors, etc.) and AliExpress (for suspected breaches in areas related to risk mitigation, etc.).

[111] Interview with Parie, Director of Algorithm Audit (Interview 13).

[112] Laguna (Deputy Head of the Commission Unit responsible for implementing the DSA), 'SNV Hintergrundgespräch: Der DSA und wie er sich durchsetzen lässt: 'Online-Talk mit Irene Roche

University of Vienna Law Review, Vol. 9 No 3 (2025), pp. 140-168, https://doi.org/10.25365/vlr-2025-9-3-140.

V. The Choice of Regulatory Instruments for the Regulation of AI and Digital Services

It can be noted that the regulatory tools of the DSA could have a potential for public oversight and for creating the conditions for broader public debates on issues such as the engagement-centred design of social media algorithms, due to ECAT but especially to the vetted researcher access.[113]

In the AI Act, the regulation of high-risk AI systems is based on *harmonised voluntary standards*, whereas oversight mechanisms and specifically the relevance of public oversight are less prominent in this regulatory regime – although this does not necessarily apply to the regulation of GPAI models. There is therefore also less room for debates on the legitimacy of the context of use of AI systems.

Both legislative frameworks demonstrate efforts to strike a balance between different regulatory goals. However, since both regulations are based in particular on internal market law (Article 114 TFEU[114]), it can be seen that the "internal market harmonisation aim"[115] is paramount. As the regulatory approach thus builds on regulatory regimes originally developed for the classical industrial economy, and as digital policy legislation brings new challenges (protection of fundamental rights and against collective-, societal harms), there is an increasing need to reduce the already existing but further growing accountability and democratic legitimacy deficits in policy making and enforcement.

Generally symptomatic of the current development of digital regulatory policy – as it can be demonstrated also in the AI Act and the DSA – are regulatory tools that are primarily directed at "risk management". Whereby they are characterised to a certain degree by a *separation of the technical from the political*. Related to this is a shift of

---

Laguna' (*Stiftung Neue Verantwortung*,16 March 2023) <https://www.stiftung-nv.de/de/publikation/transkript-zum-snv-hintergrundgespraech-der-dsa-und-wie-er-sich-durchsetzen-laesst#collapse-newsletter_banner_bottom> accessed 15 August 2023.

[113] AlgorithmWatch and AIForensics have already sent data access requests to Microsoft via the DSC to conduct research on Bing-generated election misinformation, as soon as the DSA was fully enforced (on 17 February 2024) (See Marsh and Helming, 'AlgorithmWatch and AI Forensics among the first organizations to request platform data under the DSA' (*AlgorithmWatch*, 15 February 2024) <https://algorithmwatch.org/en/dsa-platform-data-request-2024/> accessed 22 March 2024). A precise evaluation can only be made however when it becomes clear how exactly the implementation and enforcement of the AI Act is structured.

[114] Article 114 of the Treaty on the Functioning of the European Union (TFEU) provides for the adoption of measures to ensure the establishment and functioning of the internal market.

[115] Interview with official at the European Commission.

University of Vienna Law Review, Vol. 9 No 3 (2025), pp. 140-168, https://doi.org/10.25365/vlr-2025-9-3-140.

policymaking and enforcement towards "*independent institutions*" and, in part, a "*privatisation of digital policy legislation*"[116].

This can be seen in the policy-making phase for example in the importance of standard-setting processes carried out by private standard-setting bodies (as the role and the place of technical standards is crucial), or in the increase of delegated acts, which provide the Commission with more decision-making powers. In the implementation phase it is visible in the industry's responsibility for conformity assessments, risk assessments and third-party auditing, as well as in the steadily growing role of voluntary codes of conduct, and regulatory sandboxes. In general, both regulatory approaches are to a large extent based on self-assessment procedures, although in a second step auditors and/or competent national authorities as well as the Commission have an important supervisory role. This is the case for *fundamental rights impact assessments, assessments concerning high-risk classifications, risk assessments related to systemic risks of GPAI models, conformity assessments, risk assessments of VLOPs and VLOSEs.*

This development is described by a Commission official in one interview as an attempt to provide regulatory tools that are "agile and flexible", in order to deal with the speed and complexity of the regulatory issues that characterise this policy field.[117] However, these choices of regulatory instruments also show that the underpinning regulatory-/societal paradigm of the third phase in EU digital policy is to a huge degree "technological, progress driven".[118] In this sense, it is stressed in another interview by an official, that a core of this new regulatory wave is to strengthen the EU's market position vis-à-vis the US and China, through the harmonisation of the single market, so that the EU does not run the risk of becoming a "price taker" and a "technology taker".[119]

[116] See also Micklitz, 'The Role of Standards in Future EU Digital Policy Legislation - A Consumer Perspective' (2023) *Commissioned by ANEC and BEUC.*

[117] Interview with Bouwen, Policy Officer – impact assessment, at the Secretary General, European Commission (Interview 9).

[118] Smuha, 'The Human Condition in An Algorithmized World: A Critique through the Lens of 20th-Century Jewish Thinkers and the Concepts of Rationality, Alterity and History, SSRN (December 2021), http://dx.doi.org/10.2139/ssrn.4093683

[119] Interview with official at the European Commission.

VI. How to Address the Challenges of the Chosen Regulatory Instruments?

In order to achieve a better balance between the different regulatory goals (increasing productivity and competitiveness – protecting fundamental rights in the Charter – preventing collective and societal harms), some interviews suggest a stronger involvement of citizens, civil society and experts at different levels.

First, it is emphasised that participatory mechanisms could already take place at the *level of production processes* (e.g. of AI systems). This would ensure, as it is argued, that ethical considerations and normative principles shape the development of new technologies from the very beginning. Product developers would thus not be accountable for the risks of the products only when they are already on the market.[120]

Second, it is stressed by several senior officials, civil-society- and consumer interest representatives that the *levels of policy making, implementation and enforcement* of the new regulatory regimes require stronger, institutionalised participation- and, in particular, civil society engagement mechanisms. In this context, there are calls for a balanced stakeholder representation in standardisation bodies, in the various assessment procedures (e.g. fundamental rights impact assessments carried out by human rights experts), in audits (to be carried out by public organisations) and in the national competent authorities and the AI Office, the AI- and the DSA Board. In general, it is emphasised by a Commission official: "We currently see an ethics turn and it should go hand in hand with a participatory turn"[121].

Third, it is argued by several interviewees, that at the *agenda-setting level* a shift in ethics discourses to "meta-technological perspectives"[122] should take place in order to transform the contemporary technological-progress driven societal paradigm, so that the focus of digital policy could (also) go beyond the question of, for example, "how to bring ethics into the design of an AI system". This could lead to a greater awareness of which core values are about to change in this new societal era of big data, hyperconnectivity and AI and which should be protected. In this sense, an official at the Commission mentions for instance that the right to human dignity is gaining new

[120] See for example: Coeckelbergh, 'Mark Coeckelbergh on participatory democracy and artificial intelligence' (*Apple Podcasts, culturalstudies, Toby Miller)* <https://podcasts.apple.com/pl/podcast/culturalstudies/id385240141?i=1000642637495> accessed 21 March 2024.

[121] Interview with official at the European Commission.

[122] Smuha, 'The Human Condition in An Algorithmized World: A Critique through the Lens of 20th-Century Jewish Thinkers and the Concepts of Rationality, Alterity and History, SSRN (December 2021), 27, http://dx.doi.org/10.2139/ssrn.4093683

University of Vienna Law Review, Vol. 9 No 3 (2025), pp. 140-168, https://doi.org/10.25365/vlr-2025-9-3-140.

significance in the current digital transformation, as it can be linked to a new claim/right, namely to be free from the "colonialisation of human attention through engagement centric algorithms"[123]. N. Smuha argues similarly, highlighting the importance of "intersubjective relationality", which is an "essential characteristic of human existence"[124] and therefore a core value that risks being undermined in an algorithmized world where, for example, the use of AI systems in different high-risk categories is normalised, and therefore humans should have the right to its protection. Such reflections would require the creation of *open public spaces* that allow room for the development of new narratives and ethics discourses. This could ultimately lead to digital regulatory regimes that go beyond risk-based orientations, offering for instance stronger (human) rights-based approaches.

VII. Bibliography

Algorithm Audit, *White paper – Feedback on DSA Delegated Regulation (conducting independent audits)* (2023)

Bradford, A., *The Brussels effect: how the European Union rules the world* First issued as an Oxford University Press paperback ed. (Oxford University Press, 2021)

Craig, P. and G. De Búrca, *EU law: text, cases, and materials* Seventh edition ed. (Oxford University Press, 2020)

Eberlein, B. and A. L. Newman, 'Escaping the International Governance Dilemma? Incorporated Transgovernmental Networks in the European Union' (2008) 21 *Governance* 25–52

Griffin, R., 'Rethinking rights in social media governance: human rights, ideology and inequality' (2023) 2 *European law open* 30–56

Herman, K., 'Felix Stalder, The Digital Condition' (2020) *International journal of communication (Online)* 4707-

Laurent, B., *European Objects: The Troubled Dreams of Harmonization* (2022)

Micklitz, H.-W., 'The Role of Standards in Future EU Digital Policy Legislation - A Consumer Perspective' (2023) *Commissioned by ANEC and BEUC*

Savin, A., 'New directions in EU digital regulation post-2015: Regulating disruption'

[123] Interview with official at the European Commission.

[124] Smuha, 'The Human Condition in An Algorithmized World: A Critique through the Lens of 20th-Century Jewish Thinkers and the Concepts of Rationality, Alterity and History, SSRN (December 2021), 2, http://dx.doi.org/10.2139/ssrn.4093683

(2020) 11 *Pravni zapisi* 93–120

Smuha, N. A., 'The Human Condition in An Algorithmized World: A Critique through the Lens of 20th-Century Jewish Thinkers and the Concepts of Rationality, Alterity and History' (2021)

Staab, P. and T. Thiel, 'Social Media and the Digital Structural Transformation of the Public Sphere' (2022) 39 *Theory, culture & society* 129–43

Veale, M. and F. Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act — Analysing the good, the bad, and the unclear elements of the proposed approach' (2021) 22 *Computer Law Review International* 97–112

Wallace, H., M. A. Pollack, C. Roederer-Rynning, A. R. Young, H. Wallace, M. A. Pollack, C. Roederer-Rynning, and A. R. Young (eds.), *Policy-Making in the European Union* Eighth Edition, Eighth Edition ed. (Oxford University Press, 2020)

VIII. List of Interviews

Interview 1: Official, European Commission, JRC (Brussels, 18.04.2023)

Interview 2: Official, European Commission, (Online, 11.05.2023)

Interview 3: Senior Consultant, KPMG (Online, 09.05.2023)

Interview 4: Official, European Commission (Online, 10.05.2023)

Interview 5: Clément Perarnaud, Researcher at CEPS, VUB Senior Associate Researcher (Online, 16.05.2023)

Interview 6: Joachim Ott, Head of Unit, DG COMM, European Commission, DG COMM (Brussels, 17.05.2023)

Interview 7: Official, European Commission (Brussels, 01.06.2023)

Interview 8: Mark Dempsey, Senior Advocacy Officer, ARTICLE 19 (Brussels, 09.06.2023)

Interview 9: Pieter Bouwen, Policy Officer – Impact Assessment, Secretary General A2, European Commission (Brussels, 28.06.2023)

Interview 10: Senior Manager Policy & Innovation, Deputy Director-General, ANEC (Online, 24.07.2023)

Interview 11: Connor Dunlop, European Public Policy Lead, Ada Lovelace Institute (Brussels, 25.07.2023)

University of Vienna Law Review, Vol. 9 No 3 (2025), pp. 140-168, https://doi.org/10.25365/vlr-2025-9-3-140.

Interview 12: Mher Hakobyan, Advocacy Advisor on AI Regulation, Amnesty International (Online, 26.07.2023)

Interview 13: Jurriaan Parie, Director and Board member of Algorithm Audit (Online, 28.07.2023)

Interview 14: Risto Uuk, EU Research Lead at the Future of Life Institute (Online, 12.03.2024)

Interview 15: Cabinet Member - Executive Vice President Margrethe Vestager, European Commission (Online, 18.02.2024)

Interview 16: Senior Policy Expert, thinktank (Online, 25.03.2024)