ERC StG EUDAIMONIA (GA: 948473) WORKING PAPER SERIES

The Working Papers published in this series are directly based on research conducted in the framework of the ERC EUDAIMONIA project based at the University of Liège. Papers cover topics related to the different Work Packages of the project and are made available to enhance discussion even prior to formal publication of scientific articles. Comments are most welcome via *pieter.vancleynenbreugel@uliege.be*

Working Paper 2023/3

From codifying procedure to proceduralising code? – The European Union's Artificial Intelligence, Digital Services and Digital Markets Acts as instruments of cyberspace regulation and enforcement

Pieter Van Cleynenbreugel, LL.M. (Harvard), Ph.D (KU Leuven)[1]
Professor of Law, University of Liège (Belgium)
Guest professor, Université Paris-Dauphine

Key words

European Union – enforcement – digital markets – artificial intelligence – business regulation

Abstract

This paper analyses and compares the regulatory frameworks adopted or proposed by the European Union (EU) in the realm of digital services, digital markets and artificial intelligence technologies. It argues that those different frameworks are illustrative of an implicit common underlying approach towards digital regulation. Per that approach, the EU seeks to ensure digital technologies' design in compliance with its fundamental values through regulatory procedures focused on the use of technology systems and the behaviour of digital technology players. That approach, grounded in and building upon the conceptual premises of cyberspace regulation is inherently procedural. However, the way in which it has been embedded in the EU's Digital Services, Digital Markets and Artificial Intelligence Acts also highlights three fundamental limits of that procedural approach. The paper argues that in order to overcome those limits, a complementary regulatory posture in the form of proceduralising code would be

[1] This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement n° 948473). Part of this research has been conducted in the framework of the first work package of the ERC EUDAIMONIA Starting Grant project (GA n. 948473), which consists in an in-depth analysis and comparison of regulatory and enforcement arrangements in 18 fields of EU law and policy. One of those fields concerns digital markets. The arguments developed here have been developed on the basis of the groundwork done for the first WP of the project. The author can be contacted at pieter.vancleynenbreugel@uliege.be.

welcome. It subsequently calls for two steps forward in order to further develop that complementary posture within the current EU legal framework.

Word count (incl. references): 7993 words

Introduction

With the adoption of Regulations 2022/1925 (Digital Markets Act - DMA)[2] and 2022/2065 (Digital Services Act - DSA)[3], the European Union (EU) put in place a regulatory framework that explicitly targets (large) online platforms. Although both Regulations address different types of business models and behaviour, it is submitted that they indiscriminately constitute examples of a similar procedural approach to cyberspace regulation. That same approach also underlies the proposed EU Artificial Intelligence Act (AIA).[4]

This paper will unpack the premises of that procedural approach. To do so, its first part will analyse the DSA, DMA and AIA. On the basis of that analysis, the second part will identify the key features of the EU's codifying procedure ambitions prevailing in those three instruments. In its current setup, however, the EU's procedural approach is characterised by three shortcomings. In order to address those shortcomings, the paper calls for a complementary proceduralising code orientation to accompany EU codifying procedure ambitions. The currently existing EU regulatory frameworks allow for that orientation to be developed without major legal reform.

1. The EU's procedural approach to digital regulation

In adopting or proposing a new generation of digital instruments, the European Union believes that regulation is necessary to avoid digital technologies from producing unwanted effects. It is submitted that the choice to regulate is inspired by traditional debates on whether and how to regulate cyberspace (1.1.). The EU,

[2] Regulation 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 (EU) 2020/1828 (Digital Markets Act), [2022] O.J. L265/1 (hereafter DMA).
[3] Regulation 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] O.J. L277/1 (hereafter DSA).
[4] See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206 (hereafter AIA).

this paper argues, takes the basic conceptual framework undergirding cyberspace regulation as a starting point for its own particular regulatory approach common to the DSA, DMA and AIA (1.2.).

1.1. Cyberspace regulation: a conceptual framework reaching beyond the World Wide Web

The concept of cyberspace regulation emerged in the 1990s as a way to discuss and understand how negative externalities produced by the emergence of a cross-border and virtual digital environment, exacerbated by the networked structure of the Internet was to be governed. The notion encapsulates all different forms of deliberative action, both command-and-control and more cooperative manners, in the public interest, it encompasses every initiative in terms of the development and application of public or private rules aimed at addressing the infrastructure of and conduct in cyberspace.[5]

An important distinguishing feature of cyberspace – by contrast with natural resources or other types of environmental regulation – is that the underlying architecture is human-made and therefore in principle human-controlled. [6] The servers, cables, network infrastructures and the software running on them are all products of human engineering and can be influenced by them. As Lessig famously held, the architecture through which cyberspace develops – the code – is similar to the power legal norms have to enable or constrain human behaviour.[7]

Against that background, regulating cyberspace can take place on two main levels. On the one hand, regulatory efforts could focus on the technical infrastructure of cyberspace. Given the decentralised and state-transcending nature of the infrastructure involved in cyberspace, regulators generally refrain from intervening directly in the design of its infrastructure.[8] On the other hand, regulatory efforts could focus on the contents made available through the technical infrastructure cyberspace put in place. Content regulation most often relied on by public authorities on different governance levels targets specific types of activities or behaviour resulting in the production or distribution of contents

[5] J. Feick and R. Werle (2010), 'Regulation of cyberspace' in R. Baldwin (ed.), *The Oxford Handbook on Regulation* (OUP), 524.
[6] K. Yeung (2017) , 'Hypernudge: Big Data as a mode of regulation by design', *Information, Communication & Society* 20, 118-136.
[7] L. Lessig (1999), *Code and other laws of Cyberspace* (Basic Books).
[8] J. Feick and R. Werle (2010), 526.

rather than the contents themselves. Taken as a whole, content regulation in cyberspace covers an amalgam of measures that either seek to steer or influence the development of software run on the network (content design regulation) or the use made of that software by businesses or individuals (content implementation regulation). A typical example of content design regulation is intellectual property law, whereas e-commerce rules typically belong to the category of content implementation regulation. Content regulation may thus serve to avoid unwanted conduct from materializing or causing damage.[9]

The cyberspace regulation conceptual framework has been developed to justify (the need for) the regulation of the Internet. Its rationales and features also remain relevant when thinking about or developing regulatory activities covering digital technologies making use of the world wide web or the interconnectedness it enables. As a result, it is not surprising that in trying to come to terms with the regulation of those technologies, the conceptual framework coined as cyberspace regulation remains a useful starting point for regulators seeking to address, control or influence operations taking place in that space.[10]

At European Union level, the main focus of this paper, regulatory efforts have focused indeed principally on addressing contents and activities in an attempt indirectly to constrain and regulate the use of the underlying software and hardware infrastructures. That choice makes sense as the infrastructure underlying cyberspace largely transcends the territory of the European Union. However, the scope of EU cyberspace regulation is characterised by a desire to regulate contents or behaviour in order to steer the design of the underlying software and, to a lesser extent, the infrastructure necessary to distribute or develop those contents. That tendency could already be observed in the context of the adoption of the EU's General Data Protection Regulation (GDPR), which applies both to digital a non-digital processing of personal data of subjects residing in the European Union.[11] One of the consequences of that Regulation has been to steer the development of data processing activities towards EU-compliant design and practices.[12] Given the

[9] J. Feick and R. Werle (2010), 535-539.
[10] By way of example, S. Hassan and P. De Filippi (2017) , 'The Expansion of Algorithmic Governance: From Code is Law to Law is Code', *Field Actions Science Reports* [Online], Special Issue 17 , http://journals.openedition.org/factsreports/4518
[11] Regulation 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] O.J. L119/1 .
[12] A. Bradford (2020), *The Brussels Effect : how the European Union rules the world* (Oxford University Press), 132-169.

impact the GDPR has had, it should not surprise that the EU would want to replicate that instrument's underlying regulatory approach and ambitions in other fields of digital technology regulation as well.

1.2. The EU's Digital Services, Digital Markets and Artificial Intelligence Acts

The 2022 Digital Services Act (1.2.1.), the 2022 Digital Markets Act (1.2.2.) and the proposed Artificial Intelligence Act (1.2.3.) all seek to regulate digital contents or markets. By comparing their scope and provisions, they allow for a typical EU approach to digital regulation to be uncovered.

1.2.1. The Digital Services Act

The overall ambition of the Digital Services Act (DSA) is to offer professional and non-professional users of online intermediary services not only an innovative but also a safe, predictable and trusted online environment. [13] From that perspective, its provisions resemble regulations traditionally associated with consumer protection or unfair commercial practices law. The DSA obligations apply to providers of intermediary services offered to recipients that have their place of establishment or are located in the Union, irrespective of providers' place of establishment.[14] According to the DSA, intermediary services are information society services – any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services[15] – taking the form of (1) granting access to or transmitting information on a communication network ('mere conduit'), (2) transmitting information whilst also temporarily storing it on its servers (caching) or (3) transmitting information while storing it more permanently (hosting).[16] In essence, the DSA establishes a threefold regulatory framework.[17]

First, it clarifies the rules for the conditional exemption from liability of providers of intermediary services. As a matter of EU law, providers of mere conduit,

[13] Article 1(1) DSA.
[14] Art. 2(1) DSA.
[15] Article 1(1)(b) Directive 2015/1535 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] O.J. L241/1.
[16] Art. 3(g) DSA. See also Art. 2(2) DSA: it only applies to intermediary services and not to any other service, even when the latter is provided through an intermediary service.
[17] As also indicated in Article 1(2) DSA.

caching and hosting services are not exempted from liability for illegal contents transmitted via them.[18] The DSA confirms the earlier regime featured already in a 2000 EU Directive.[19] The DSA nevertheless adds that no general obligation to monitor the information which providers of intermediary services transmit or store, nor actively to seek facts or circumstances indicating illegal activity shall be imposed on those providers.[20] It thus means that online platforms and other transmitting services are not obliged to monitor and, if necessary, moderate, all contents in a general and anticipatory manner. However, the DSA does put in place a mechanism for collaboration with administrative or judicial authorities. Upon request, services providers have to provide information or take measures to remove illegal content. The Act outlines particular cooperation obligations with competent authorities in that regard.[21]

Second, the DSA contains rules on specific due diligence obligations tailored to certain specific categories of providers of intermediary services. Overall, the DSA calls for codes of conduct and voluntary 'good digital governance' standards to be put in place.[22] In addition, four incremental layers of due diligence procedures and obligations are imposed on service providers, which increase depending on the role the provider plays in storing transmitted information.

In the first layer of regulatory obligations, all intermediary services providers need to have a point of contact or legal representative in the European Union.[23] Their terms and conditions need to include information on any restrictions that they impose in relation to the use of their service.[24] In addition, they have to make publicly available at least once a year a report on requested or self-initiated content moderation initiatives.[25]

As part of the second layer of obligations, providers of hosting services have to put in place additional notice and action mechanisms. Those mechanisms should allow any individual or entity to notify them of the presence on their service of

[18] Art. 12-15 Directive 2000/31 f 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'), [20000] O.J. L178/1.
[19] Art. 5(1)(e) and 6(1)(b) DSA.
[20] Art. 8 DSA.
[21] Art. 9-10 DSA.
[22] Art. 44-48 DSA.
[23] Art. 11-13 DSA.
[24] Art. 14 DSA.
[25] Art. 15 DSA.

specific items of information that the individual or entity considers to be illegal content.[26] Upon becoming aware of information giving rise to suspecting a criminal offence involving a threat to the life or safety of a person or persons, hosting service providers are obliged to inform competent authorities and provide all information available so that those authorities can take appropriate action.[27] When the provider takes decisions to remove content or suspend activities from a service user, it needs to motivate in a comprehensible and detailed manner the reasons and grounds for that action.[28]

The third layer of regulatory obligations extends to online platforms, which are defined as hosting services that, at the request of a recipient of the service, store and disseminate information to the public.[29] Those online platforms have to recognise and give priority to requests for content moderation introduced by 'trusted flaggers', organisations which have been recognised by public authorities for their independence from the platforms concerned and their particular expertise and competence for the purposes of detecting, identifying and notifying illegal contents.[30] In addition, online platforms have to provide for an internal complaint-handling mechanism[31], a certified out-of-court settlement system[32] and procedures to allow actions against misuse of complaints.[33] In addition, its web interface cannot mislead users and advertisements clearly have to be distinguished from the actual information hosted on the platform[34] and mechanisms to protect the safety of minors using the services have to be in place.[35] When using recommender systems, the platform's terms and conditions have to explain, in plain and intelligible language, the main parameters used in their recommender systems, as well as any options for the recipients of the service to modify or influence those main parameters.[36] For online platforms that allow consumers to conclude distance contracts with traders, those traders must be traceable and the interface must be designed so that traders can comply with all pre-contractual obligations (compliance by design) related to the conclusion of distance

[26] Art. 16 DSA.
[27] Art. 18 DSA.
[28] Art. 17 DSA.
[29] Art. 3(i) DSA.
[30] Art. 22 DSA.
[31] Art. 20 DSA.
[32] Art. 21 DSA. That system does not prejudice to the right of the recipient of the service concerned to initiate, at any stage, proceedings to contest those decisions by the providers of online platforms before a court in accordance with the applicable law.
[33] Art. 23 DSA.
[34] Art. 25-26 DSA.
[35] Art. 28 DSA.
[36] Art. 27 DSA.

contracts.[37] Consumers shall also be informed of illegal products sold via their intermediary.[38] Again, online platforms have to publish reports in which their actions are outlined.[39]

The fourth and final layer of regulation concerns very large online platforms as well as very large online search engines, i.e. those platforms or engines that have more than 45 million users in the European Union.[40] Those very large operators, which have to pay a yearly supervisory fee to the European Commission[41], have to diligently identify, analyse and assess any systemic risks in the Union stemming from the design or functioning of their service and its related systems, including algorithmic systems, or from the use made of their services.[42] That risk assessment obligation constitutes a starting point for risk mitigation measures that have to be taken by those platforms and search engines. Those measures may include adaptations to algorithms used, to content moderation processes, to the design of the interface and other measures the platform can introduce to ensure compliance with the DSA. [43] Very large online platforms additionally have to commission independent audits of their functioning[44], have an internal compliance function in place[45] and abide by additional transparency obligations with regard to advertising featuring on their interfaces.[46] For each recommender system used, they have to offer one option not based on profiling.[47] Again, a detailed and publicly available report on measures taken has to be published annually.[48] In times of systemic crisis, the European Commission may require very large online platforms and search engines to take crisis measures to avoid that systemic threats to public security or public health in the EU will materialise. The platform concerned can decide on what measures to take, but the Commission will actively monitor what measures are taken.[49]

Third, the DSA also sets out, in a detailed manner, rules on the implementation and enforcement of this Regulation, including as regards the cooperation of and

[37] Art. 30-31 DSA.
[38] Art. 32 DSA.
[39] Art. 24 DSA.
[40] Art. 33(1) DSA.
[41] Art. 43 DSA.
[42] Art. 34 DSA.
[43] Art. 35 DSA.
[44] Art. 37 DSA.
[45] Art. 41 DSA.
[46] Art. 39 DSA.
[47] Art. 38 DSA.
[48] Art. 42 DSA.
[49] Art. 36 DSA.

coordination between the competent authorities. More particularly, the DSA requires Member States to set up new independent authorities which are called Digital Services Coordinators.[50] The DSA determines their powers, procedures and command-and-control enforcement and sanctioning powers.[51] Individuals have the right to lodge a complaint with the Coordinator, which has to inform them on the follow-up given to it, but is not forced to act upon the complaint.[52] Those individuals may also claim compensation for harm caused by intermediary services providers.[53] The different Coordinators form part of a European Digital Services Board, which coordinates joint investigations and mutual assistance between different Coordinators and may call upon the Commission to recommend further enforcement measures being taken by a Member State Coordinator.[54] The European Commission for its part is responsible for monitoring very large online platforms. The DSA confers it inspection and sanctioning powers and judicial review possibilities against Commission enforcement decisions.[55] For all enforcement actors involved, professional secrecy and information sharing obligations have been added as well.[56]

1.2.2. The Digital Markets Act

By contrast with the DSA's consumer or unfair commercial practices focus, the Digital Markets Act (DMA) is an instrument that aligns more closely with competition law rules.[57] The DMA seeks to lay down harmonised rules ensuring for all businesses, contestable and fair markets in the digital sector across the Union.[58] To do so, it imposes a regulatory regime on core platform services provided or offered by so-called gatekeepers to business users established in the Union or end users established or located in the Union, irrespective of the place of establishment or residence of the gatekeepers and irrespective of the law

[50] Art. 49 DSA.
[51] Art. 50-52 and 55-56 DSA.
[52] Art. 53 DSA.
[53] Art. 54 DSA.
[54] Art. 61-63 and 56-60 DSA.
[55] Art. 65-83 DSA.
[56] Art. 84-85 DSA.
[57] N. Moreno Belloso and N. Petit, 'The EU Digital Markets Act (DMA) : A Competition hand in a regulatory glove ?', *European Law Review* (2023), forthcoming, draft paper available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4411743. The competition law resemblance does not mean that EU or national competition law rules no longer apply to businesses falling under the DMA, see also Art. 1(6) DMA. However, EU Member State authorities may not adopt decisions running counter to European Commission decisions adopted under the DMA, see Art. 1(7) DMA.
[58] Art. 1(1) DMA.

otherwise applicable to the provision of service.[59] The DMA defines the notion of gatekeeper and submits them to increased regulatory scrutiny, backed up by command-and-control measures.

First, the DMA applies to undertakings having gatekeeper status.[60] An undertaking is an entity engaged in an economic activity, regardless of its legal status and the way in which it is financed, including all linked enterprises or connected undertakings that form a group through the direct or indirect control of an enterprise or undertaking by another.[61] Such undertakings shall be designated as a gatekeeper if they provide a core platform service which is an important gateway for business users to reach end users. Core platform services are listed exhaustively in the DMA. They concern the following activities or actors : online intermediation services, online search engines, online social networking services, video-sharing platform services, number-independent interpersonal communication services, operating systems, web browsers, virtual assistants, cloud computing services and online advertising services.[62] To further qualify as a gatekeeper, a core platform service provider has to have a significant impact on the EU's internal market. According to the DMA, that is the case where it achieves an annual Union turnover equal to or above EUR 7,5 billion in each of the last three financial years, or where its average market capitalisation or its equivalent fair market value amounted to at least EUR 75 billion in the last financial year, and it provides the same core platform service in at least three Member States. Gatekeeper status also requires that the undertaking concerned enjoys an entrenched and durable position, in its operations, or it is foreseeable that it will enjoy such a position in the near future. According to the DMA, that would be the case when the abovementioned turnover or capitalization values would be met in each of the last three financial years.[63] Undertakings that meet those thresholds have to inform the European Commission of their presumed gatekeeper status.[64] Within 45 working days, the European Commission will then adopt a decision establishing the undertaking concerned as a gatekeeper.[65] However, the DMA

[59] Art. 1(2) DMA
[60] Art. 3 DMA.
[61] Art. 2(27) DMA. See also CJEU, 23 April 1991, C-41/90, *Höfner*, EU:C:1962:31, para. 21.
[62] Art. 2(2) DMA. The European Commission can conduct a market investigation with a view to include other digital services to the list of core platform services, Art. 19 DMA.
[63] Art. 3(2) DMA. An undertaking providing core platform services shall not segment, divide, subdivide, fragment or split those services through contractual, commercial, technical or any other means in order to circumvent the quantitative thresholds, see Art. 13 DMA.
[64] Art. 3(4) DMA.
[65] Art. 3(5) DMA.

makes it possible for the undertaking to adduce reasons why it should not be considered a gatekeeper. If serious arguments are offered, the European Commission will have to conduct a market investigation on the basis of which it may or may not conclude to gatekeeper status.[66] In the same way, when not all the turnover, capitalization or entrenched position conditions are met, the European Commission may still conclude to gatekeeper status on the basis of a market investigation, taking into account structural business or services characteristics.[67] One undertaking can be designated a gatekeeper for one or more core platform services.[68]

Second, once designated a gatekeeper, the undertaking concerned must comply with regulatory obligations set out in the DMA. Those obligations include limitations on the use of personal data for advertisement purposes, taking measures to allow users to commercialise their products through third parties or giving users the ability to carry over their data to another platform.[69] The obligations have been laid out in a fairly detailed fashion in the DMA. Gatekeepers are expected to ensure and demonstrate compliance with those different obligations.[70] The European Commission can decide preliminarily to assess the effectiveness of proposed measures or could adopt a decision specifying how certain obligations have to be put in operation.[71] In exceptional circumstances, the respect for the obligations concerned may be suspended.[72] The European Commission could also, on grounds of public security or public health, decide to exempt an undertaking from complying with certain obligations imposed by the DMA.[73] The designation of a gatekeeper thus sets in motion a process of regulatory dialogue between the European Commission and the undertaking concerned. The latter has to report at least once a year how it complies with the DMA[74] and is obliged to undergo an independent audit within 6 months after being designated a gatekeeper.[75] Gatekeepers also have to introduce a compliance function that can liaise directly with the European Commission.[76]

[66] Art. 17 DMA.
[67] Art. 3(8) DMA.
[68] Art. 3(9) DMA.
[69] Art. 5-7 DMA.
[70] Art. 8(1) DMA.
[71] Art. 8(3) DMA.
[72] Art. 9 DMA.
[73] Art. 10 DMA.
[74] Art. 11-12 DMA.
[75] Art. 14 DMA.
[76] Art. 28 DMA.

Third, not unlike the DSA, the DMA contains an elaborate command-and-control investigation and decision-making framework aimed at addressing non-compliance with the regulatory obligations. The European Commission has been designated as the regulatory body in charge of such investigations. It has been given the power to request information, to take statements, to order inspections, to take interim measures and to turn commitments offered by gatekeepers into binding decisions.[77] In case of non-compliance, the European Commission must adopt a decision opening proceedings[78], which in turn could result in a non-compliance decision.[79] That decision may be accompanied by the imposition of fines of maximum 10% of un undertaking's worldwide turnover.[80] Failure to collaborate with the Commission may result in periodic penalty payments being imposed.[81] The DMA additionally empowers the European Commission to take any behavioural or structural remedy decision – including splitting up undertakings – in cases of systematic non-compliance and on the basis of a market investigation. Systematic non-compliance occurs where the Commission has issued at least three non-compliance decisions against a gatekeeper in relation to any of its core platform services within a period of 8 years prior to opening of the market investigation. The European Commission could only take measures that are proportionate and necessary to ensure compliance with the Regulation.[82]

1.2.3. The EU's Artificial Intelligence regulatory framework in-the-making

In addition to the DSA and the DMA, the European Commission has proposed a regulatory framework to be adopted in relation to artificial intelligence. That framework, which is covered by a proposed Artificial Intelligence Act (AIA) and Directives on the topic of liability for harm caused[83], seeks to impose EU-style product safety regulations on AI products used within the territory of the European Union. In its present setup, it resembles the procedure-focused approach also underlying the DSA and DMA. In what follows, this paper focuses on the

[77] Art. 21-27 DMA.
[78] Art. 20 DMA.
[79] Art. 29 DMA.
[80] Art. 30 DMA.
[81] Art. 31 DMA.
[82] Art. 18 DMA.
[83] For an overview, https://commission.europa.eu/business-economy-euro/doing-business-eu/contract-rules/digital-contracts/liability-rules-artificial-intelligence_en.

proposal introduced by the European Commission in 2021 and amended by the Member States in the Council in November 2022.[84]

The AIA proposal targets primarily providers and users of AI systems that operate in the European Union.[85] AI systems are defined as systems designed to operate with elements of autonomy and that, based on machine and/or human-provided data and inputs, infers how to achieve a given set of objectives using machine learning and/or logic- and knowledge-based approaches, and produces system-generated outputs such as content (generative AI systems), predictions, recommendations or decisions, influencing the environments with which the AI system interacts.[86] In essence, the AIA is characterised by three complementary regulatory layers, which focus predominantly on so-called high risk AI systems.

First, the AIA proposes a classification of AI systems based on the risk their use poses. If adopted, the Act would therefore not seek to regulate directly the development of AI systems, but rather their use in the territory of the European Union. To do so, it requires AI systems to be classified and assessed prior to being used. The Act distinguishes between unacceptable risk, high-risk and minimal risk systems.

As a starting point, AI systems posing unacceptable risks are prohibited from being used in the European Union. According to the AIA, are prohibited AI systems that (1) rely on subliminal techniques beyond a person's consciousness in order to materially distort a person's behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm, (2) that exploit any of the vulnerabilities of a specific group of persons due to their age, physical or mental disability, (3) are used by public authorities or private actors to give a 'social score' to individuals that may result in unfavourable or detrimental treatment of individuals or groups and (4) use real time remote biometrical information for the purposes of law enforcement not related to terrorism or life-threatening behaviour.[87]

[84] See for that version of the text, https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/.
[85] Art. 2(1) AIA. Military, defence and national security systems as well as research and development activities fall outside the scope of the Act, see Art. 2(3) and (6).
[86] Art. 3(1) and recitals 6 – 6d AIA.
[87] Art. 5 AIA.

Next, AI systems that are high-risk in nature, may be used only when complying with stringent regulatory requirements. The AIA defines high-risk AI systems as any product or safety component that, in accordance with EU product safety legislation, already needs to undergo conformity assessments prior to being offered on the EU market.[88] Annex III to the AIA additionally states that are high risk, systems used for (1) remote biometric identification, (2) the management and operation of critical infrastructure such as road traffic, digital infrastructure and the supply of water, gas, heating and electricity, (3) the purpose of determining access or assigning natural persons to educational and vocational training institutions or for assessing them, (4) the recruitment, promotion or termination of workers, (5) evaluating the eligibility of natural persons for public assistance benefits and services, their creditworthiness or the price for life or health insurances, or the priority in terms of first emergency responses, (6) supporting or analysing law enforcement practices, including profiling, (7) migration, asylum and border management and (8) assisting a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts. The list does not mention explicitly generative AI such as ChatGPT, which can have multiple purposes in practice, raising the question as to whether this system would fall in this category under the currently proposed Act.[89] When adopted, the European Commission would nevertheless be able to add categories to the high-risk list annexed to the Act.[90] The AIA complementarily also lists that general purpose AI systems that may be used as a high-risk system would need to comply with the requirements imposed on specific high-risk systems, in accordance with the modalities to be determined by an implementing act.[91] A general purpose system is an AI system that is intended by the provider to perform generally applicable functions such as image and speech recognition, audio and video generation, pattern detection, question answering, translation and others. Such a system could be used in a plurality of contexts and be integrated in a plurality of other AI systems.[92]

Finally, the AIA also refers to AI systems posing limited or minimal risk. This residual category of AI systems includes all systems that are not considered to be of unacceptable or high risk. To the extent that they are intended to interact with

[88] Art. 6 AIA.
[89] See https://www.politico.eu/article/eu-plan-regulate-chatgpt-openai-artificial-intelligence-act/.
[90] Art. 7 AIA.
[91] Art. 4(b) AIA.
[92] Art. 3(1)(b) AIA.

natural persons, emotion recognition systems and biometric categorisation systems, and AI systems used to generate or manipulate image, audio or video content, their use needs to respect all conformity and commercialisation requirements imposed on similar, non-AI products seeking EU market access. The AIA imposes particular additional transparency obligations on them.[93]

Second, the AIA provides a detailed conformity assessment and market monitoring framework for high-risk AI systems. Any high-risk system has to be accompanied by a risk management strategy[94], appropriate technical documentation[95], data governance features[96], transparency towards users[97], accuracy, cybersecurity and robustness guarantees[98], record-keeping facilities[99] and tools guaranteeing human oversight.[100] The AIA does not prescribe exactly how each system needs to guarantee those values, but leaves it to providers ans users to ensure that compliance with them is ensured.[101] The providers and users of those systems would have to undergo conformity assessments prior to the use of the system and will be subject to intensive market monitoring mechanisms as well.[102] Providers have to put in place a quality management system[103], keep automatically registered logs of the system's activities[104], must undertake corrective action directly when necessary[105] and cooperate actively with national authorities.[106] Both manufacturers and providers of a system are responsible for its compliance with the Act.[107] Importers, distributors or other third parties can be considered providers in the meaning of the AIA when they add their trademark to a system or substantively modify it.[108] Users for their part would have to operate and monitor the system in accordance with its instructions for use and must also keep an automatically generated log of operations. The user nevertheless would

[93] Art. 52 AIA.
[94] Art. 9 AIA.
[95] Art. 11 AIA, to be drawn up by providers, see Art. 18 AIA.
[96] Art. 10 AIA.
[97] Art. 13 AIA.
[98] Art. 15 AIA.
[99] Art. 12 AIA.
[100] Art. 14 AIA.
[101] Art. 8 AIA.
[102] Art. 16 and 19 AIA.
[103] Art. 17 AIA.
[104] Art. 20 AIA.
[105] Art. 21 AIA.
[106] Art. 22-23 AIA.
[107] Art. 24 AIA.
[108] Art. 23(a) and 25-27 AIA.

have discretion in organising its own resources and activities for the purpose of implementing the human oversight measures indicated by the provider.[109]

Third, the AIA also contains detailed rules on how conformity assessments, monitoring and market surveillance in relation to high risk AI systems are to take place. It outlines in detail the conformity assessment procedures and standard-setting mechanisms to be conducted by notified bodies authorised by notifying authorities.[110] In addition, Member States' market surveillance authorities are empowered to monitor compliance with the Act once AI systems have been given market access.[111] This may result in measures to withdraw the system from a national market. The European Commission may be called upon to verify the justified nature of such measures.[112] The AIA also requires Member States' supervisory authorities to impose sanctions in cases of non-compliance.[113] Those authorities would need to be provided with a sufficient number of personnel permanently available whose competences and expertise span both AI and fundamental rights.[114] The different authorities meet together with the European Commission, which can issue guidelines on the AIA's implementation and application[115], in the context of an advisory European Artificial Intelligence Board.[116]

2. From codifying procedure to proceduralising code?

In adopting the DSA, DMA and in proposing the AIA, the European Union institutions have opted for a dense procedural framework of regulation backed up by command-and-control regulatory techniques. That framework can framed as being built on a codifying procedure approach to digital technologies' regulation (2.1.). In essence, that approach aims to make sure that designers and users of technologies comply with the values the EU as a regulatory regime holds dear. As a result, codifying procedure serves as a means to ensure that the code or architecture of the technologies concerned in EU value-compliant. This section argues that, despite its good intentions, this regulatory method is characterised by

[109] Art. 29 AIA.
[110] Art. 30-51 AIA. Art. 33a confirms the existence of a presumption of conformity for AI designed in accordance with EU harmonised standards.
[111] Art. 61-68b AIA.
[112] Art. 66 AIA.
[113] Art. 71 AIA.
[114] Art. 59(4) AIA.
[115] Art. 58(a) AIA.
[116] Art. 56 and 58 AIA.

three pitfalls that may render the ambition to arrive at value-compliant codes difficult to attain (2.2.). To the extent that the European Union is serious about taking such matters, it is submitted that the procedural focus it has taken would have to be extended to the field of technology designs as well. By adopting a complementary and more explicit proceduralising code approach, we believe that the identified pitfalls' effects could be mitigated and the EU's regulatory ambitions achieved more successfully (2.3.).

2.1. Codifying procedure as an underlying common regulatory approach

Despite their different focuses and ambitions, it is submitted that the EU's regulatory frameworks underlying the DSA, DMA and AIA reflect a common procedural approach to digital regulation. That approach is centred on three premises: (1) an overall preference for indirectly regulating substance through procedure, (2) increasing regulatory dialogue in the implementation phase and (3) a subsidiary focus on (and threat of) command-and-control enforcement.

First, with the exception of some plain prohibitions (such as unacceptable risk AI systems in the AIA and the list of 'gatekeeping' practices in the DMA), the overall consequence of the DSA, DMA and AIA has been to set up a framework putting in place procedures (such as reporting obligations in the DSA, DMA and AIA or audit obligations for very large online platforms or gatekeepers) with a view to make sure online platforms and artificial intelligence users respect implicit external ethical standards (diligent behaviour in the DSA, unfair practices in the DMA, transparency, accuracy and risk management in the AIA) that underpin key normative values the EU holds dear.[117] Rather than imposing directly certain design or operational requirements on platforms or AI technologies, the regulatory instruments put in place a framework through which operators or users are able to induce that their practices are in conformity with those (somewhat implicit) standards.[118]

Second, the procedural framework put in place leaves room for what could be called regulatory dialogue, i.e. discussions or talks between the

[117] Such a framework seems inspired by systems theory and cybernetics, see R. Nobles and D. Schiff (2012), *Observing law through systems theory*, Hart Publishing.
[118] M. Finck (2018), 'Digital co-regulation: designing a supranational legal framework for the platform economy', *European Law Review* 33-67.

regulator/supervisor and the supervisees.[119] Rather than immediately imposing traditional sanctions (administrative fines or criminal sanctions), technology operators are given the opportunity to justify themselves and to demonstrate how they comply with the obligations imposed on them. The EU in that regard clearly favours a co-regulatory approach in which it sets itself the framework, but leaves a certain leeway for technology operators to demonstrate compliance with the regulatory obligations in place.[120] Testament to the co-regulatory approach towards regulation, the European Union requires a dialogical process to be maintained during risk mitigating or compliance by design operations (DSA), market investigations (DMA) or conformity or market monitoring assessments (AIA). That process requires the active cooperation and participation of actors using or introducing digital technologies. In practice, this will require constructive and ethical working relationships to be set up between regulators and supervisees. The different EU regulatory instruments all seem to assume those relationships will and can be forged[121], especially because of the ultimate and subsidiary threat of sanctions lingering in the background.

Third, the EU regulatory frameworks adopted or proposed do promote cooperation with supervisees, but do not exclude the possibility of command-and-control enforcement in case of non-compliance either. As a result, the different regulatory instruments contain detailed procedures outlining how EU rules can be enforced against unwilling supervisees. In proposing those sanction mechanisms as back-up tools to ensure compliance, the EU regulations make clear that the process of good cooperation they require from supervisees is not at all voluntary. Sincere cooperation within the regulatory dialogue procedure may avoid triggering the non-compliance enforcement procedures, but the threat of the latter being activated remains always lingering in the background.

As a consequence, all three regulatory instruments take very seriously the introduction of harmonised, streamlined and coordinated principal dialogical co-regulation and subsidiary command-and-control enforcement procedures. It does not seem exaggerated to argue that the key focus of the different instruments is on

[119] J. Black (2002), 'Regulatory conversations', *Journal of Law & Society*, 163-196.
[120] P. Van Cleynenbreugel (2021), "EU By-Design Regulation in the Algorithmic Society: A Promising Way Forward or Constitutional Nightmare in the Making?" in Constitutional *challenges in the algorithmic society*, eds. O. Pollecino, et al., Cambridge University Press, 202-218.
[121] For a more skeptical general perspective (outside the field of digital regulation), already J. Black (2001), 'Proceduralising Regulation : Part II', *Oxford Journal of Legal Studies*, 33-58.

codifying cooperative and command-and-control regulatory and enforcement procedures.

2.2. The pitfalls of codifying procedure

The analyses of the DSA, DMA and AIA indicate that the EU believes that the best way forward in ensuring compliance with key substantive standards of diligence, decency, fairness and accuracy is by setting up a procedural framework in which discussions or enforcement actions focused on those values can take place. Rather than imposing on technology operators an obligation to design technologies in a certain value-compliant manner, room is left for those operators to design technologies and to integrate those values as they deem fit.[122] In that understanding, the EU regulations thus adopted or proposed would constitute a mere intermediate step towards arriving at ethical and compliant digital technologies. Despite having put in place an extensive procedural and regulatory dialogue framework, we submit that the EU's 'codifying procedure' focus' suffers from three deficits in its current setup. Those deficits would risk, in the longer term, to hamper the effectiveness and ambitions the EU legislator set for itself.

First, the procedural framework put in place is in essence inductive. Although the recitals accompanying the legal instruments indicate to some extent what substantive ethical values are being protected, the actual standards against which the European Union would hold designers, developers and users of digital technologies (code) remain vague. In the DSA, DMA and AIA, it is clear that the procedures set up are meant to enable a dialogue on how value-compliant digital technologies can be set up. However, at the outset, the values and the ways in which the EU regulator understands them or needs to understand them are absent to a large extent. Despite significant attention to different procedural steps and developments, this bears the risk of substantive opaqueness. A more explicit underlying substantive value framework in place would be helpful, if only to give the necessary tools to the regulators to evaluate the legality of the digital activities concerned.[123] In the context of artificial intelligence, that is the case to some extent with the ethics guidelines laid out by an expert group designated by the European Commission.[124] Those guidelines effectively outline what the European

[122] By way of an explicit example, Art. 31 DSA, which requires compliance by design from online platforms.
[123] For that perspective, G. Teubner (1993) , *Law as an autopoietic system*, Blackwell, 64-99.
[124] For background, see N. Smuha (2019) , 'The EU approach to ethics guidelines for trustworthy artificial intelligence', *Computer Law Review International*, 97 – 106.

Commission understands by ethical AI within the European Union. Although not explicitly mentioned as such in the AIA text, it is therefore expected that those guidelines will constitute the implicit substantive benchmarks against which assessment and monitoring procedures would be conducted. By contrast, in the framework of digital services and digital markets, a clearer frame on what is considered good behaviour and what may trigger regulatory scrutiny seems largely absent, apart from a series of gatekeeping practices considered problematic. As a result, both instruments hold the risk of remaining procedural frameworks operating through a substantive law black box.

Second and related, the procedures put in place allow regulators above all to respond to issues that are of a non-systemic manner. The behaviour of digital services providers, gatekeepers or specific artificial intelligence software is being monitored and addressed by means regulatory dialogue and command-and-control measures. Those measures may have as a consequence that individual problems are addressed and focused on. As a result, systemic threats caused by digital developments may be overlooked. The different regulations are aware of the need to take a systemic perspective on regulating digital technologies. However, their focus remains on the behaviour major systemic market operators and their impact on the functioning of the digital sphere. Systemic limits to or consequences for the infrastructure or code that may also take place are not the key focus of the regulatory regimes put in place. The regimes that have been set up or proposed would leave too little room for a fundamental reflection process on what it is exactly EU digital regulation wants to protect.

Third, on a more practical level, the regulatory regimes put in place require a lot of regulatory and enforcement capacities of both EU and Member State regulatory bodies. In the case of the DSA and AIA, new authorities would have to be created for that purpose. Questions can be raised in that regard as to whether the capacity-building presumed present can be expected to be in place from the start. In order for Member States' regulatory bodies to acquire a sufficient amount of expertise, some years of experience in regulating and dealing with relevant digital technologies or actors would seem to be necessary. In addition, absent a more explicit substantively grounded ethics or value framework against which behaviour of digital operators can be assessed, the application and implementation of newly established procedure-focused regulatory frameworks may quickly meet its limits.

2.3. Proceduralising code as a necessary complement ?

The previous section argued that the lack of clear substantive law standards against the background of which regulatory dialogue takes place, risks hampering the effective application of the new regulatory frameworks the EU has put in place or proposed. It is therefore submitted that, in order fully to arrive at a workable regulatory framework, a complementary and more substantive law-oriented background framework would contribute to the effective enforcement and application of those new regulations. That framework would ideally have to determine – and to some extent operationalise – the values in accordance with which digital technologies have to be designed or coded into digital technologies (hence the reference to code). Having such a framework in place would also increase legal certainty and compliance and enable businesses to become or remain active on the EU market in the best circumstances possible.

To the extent that the EU favours a procedural approach centred on regulatory dialogue, nothing would impede to envisage a similar approach to discuss and establish the substantive values that would have to be embedded in digital technologies' designs. Such a procedural – or proceduralising code – approach has already taken place in the context of Artificial Intelligence regulation but could, in our opinion, also be extended to other types of digital regulation in order to avoid the pitfalls outlined above. The AIA shows that it is perfectly possible to organise this within the current EU law framework. In that understanding, a proceduralising code framework in EU law contains two key steps.

A first step could be to make explicit in a more formal manner the substantive values regulation seeks to attain. This could be referred to as substantive value benchmarking. Benchmarking of relevant values could result from a wide consultation and debate process. At the EU level, the setting up of an expert group and of a debate regarding AI ethics standards serves as an example. Setting out substantive law values that serve as benchmarks for regulatory dialogues the EU seeks, at the very least diminishes the pitfalls outlined above. It would therefore be preferable should a similar exercise be conducted in the context of digital services and digital markets as well, concomitantly with the implementation of the DSA and DMA.

It is submitted that the mere existence of a substantive value catalogue is not sufficient. A second step necessary would be to allow designers to experiment with the implementation of those values when setting up technologies or platform offerings within the European Union. Once again, the AIA contains the grains for this approach by allowing for 'regulatory sandboxes' to develop.[125] Such sandboxes would offer a controlled environment in which the development, testing and validation of innovative digital systems can take place for a limited time before their placement on the market under the direct supervision and guidance by the competent authorities.[126] It remains to be seen whether and how that sandbox approach will develop in practice, but its inclusion in the AIA shows that the EU appears willing to take a proceduralising code step forward. It can only be hoped that similar regimes will accompany the DSA and DMA in the near future.

The two steps outlined here towards a more developed proceduralising code framework would, in our opinion, not as such offer a guarantee for effective regulatory oversight. To achieve that, sufficient capacity-building and experience will need to come in place in the first years after the entry into force of the new regulatory frameworks. However, having them in place as a complement to regulatory dialogue procedures as envisaged by the DSA, DMA and AIA would seem to be necessary in order to give the EU's codifying procedure regulatory approach at least a chance of contributing to more ethically designed digital technologies within the EU. The AIA shows that the EU legislator could perfectly take such steps. As a result, their integration in the DSA and DMA frameworks as well would be most welcome.

Conclusion

This paper analysed and compared three instruments of digital regulation (DSA, DMA and AIA) adopted or proposed by the European Union. Despite their different ambitions and contents, they all reflect a common underlying regulatory approach, which consists in imposing regulatory dialogue procedures backed up by command-and-control mechanisms on digital market operators. However, this paper argued that, absent clear substantive law benchmarks determining how digital technologies have to be designed or coded, the procedural framework in

[125] W. Johnson (2023), 'Caught in quicksand? Compliance and legitimacy challenges in using regulatory sandboxes to manage emerging technologies', *Regulation & Governance,* https://doi.org/10.1111/rego.12487.
[126] Recital 72, Art. 3(52) and Art. 53-54 AIA.

place risks becoming of limited value. It therefore proposed to complement that regulatory approach with a proceduralising code complement, that would use regulatory dialogue better to benchmark substantive law standards and to introduce regulatory sandboxes as a software design strategy. The AIA seems to be most advanced in that regard. It is submitted, however, that for the DSA and DMA to be enforced effectively, benchmarking and sandboxing may constitute constructive ways forward to complement the EU's codifying procedure approach.