CEPS IN-DEPTH ANALYSIS

THE AI ACT AND EMERGING EU DIGITAL *ACQUIS*

Overlaps, gaps and inconsistencies

Artur Bogucki, Alex Engler, Clément Perarnaud, Andrea Renda

September, 2022 - 02

SUMMARY

The European Commission's proposed Artificial Intelligence (AI) Act attempts to regulate a wide range of AI applications, aligning them with EU values and fundamental rights through a risk-based approach. The scope, instruments and governance framework introduced by the proposal are still being debated and refined by European co-legislators. Both the Council of the European Union and the European Parliament have proposed possible amendments to the regulation, with potentially far-reaching impacts on its overall scope and content. An agreement seems possible by mid-2023, but this will depend on whether the co-legislators converge on key issues such as the definition of AI, the risk classification and associated regulatory remedies, governance arrangements and enforcement rules.

The act has been presented as a 'horizontal' piece of legislation, even if several limitations and exemptions apply. This, combined with the expected, pervasive impact of AI on the economy and society, may lead it to overlap with several legislative provisions – both horizontal and sector specific. As a result, gaps and inconsistencies may emerge that negatively affect legislative quality and regulatory certainty. This study addresses this issue by analysing the interplay between the AI Act and EU digital *acquis*. We map the gaps and limitations of the AI Act in relation to 14 pieces of legislation. Our research draws on desk research, qualitative interviews and an online workshop.

We identify eight key areas where challenges may emerge, and make the following policy recommendations: 1) there is a need to clarify and align the terminology with the legal categories and notions in existing EU legislation related to AI; 2) negotiators should ensure better fine-tuning of the interactions of the act with sector-specific rules (notably in the health sector); 3) the act should be made consistent with EU data protection rules, for example regarding the lawfulness of personal data processing; 4) the act's risk-based approach features a number of loopholes that need to be addressed to improve legal certainty for AI providers and users; 5) while the act aims to complement existing product safety rules, it requires more detailed provisions to allow for meaningful integration with EU *acquis*; 6) the act introduces a weak enforcement scheme, which should be strengthened and aligned with other digital policies; 7) EU legislators should tackle the growing divergence between the stated goals of the act and emerging data transfer rules; and 8) the act would benefit from exemptions aimed at promoting scientific research.

Artur Bogucki is a Research Assistant at CEPS, Alex Engler is a Fellow in Governance Studies at The Brookings Institution, Clément Perarnaud is a Researcher in the Global Governance, Regulation, Innovation, Digital Economy (GRID) unit at CEPS and Andrea Renda is a Senior Research Fellow and Head of Global Governance, Regulation, Innovation and the Digital Economy (GRID) at CEPS.

This study received funding support from the Future of Life Institute.

CEPS • Place du Congrès 1 • B-1000 Brussels • Tel: (32.2) 229.39.11

CONTENTS

INTRODUCTION

The recent proposal by the European Commission for a new Artificial Intelligence Act (AI Act) is an important legislative development, illustrating the ongoing acceleration of the European Union's efforts to regulate digital technologies and services. Now under discussion both in the European Parliament (EP) and in the Council of the EU, this proposal is a much-awaited attempt by the European executive to regulate a wide range of AI applications and products, bringing them in line with EU values and fundamental rights through a risk-based approach.

As negotiations are still ongoing at EU level, the scope, instruments and governance framework introduced by the proposal are still being debated and refined by European legislators, with a view to finalising the text by mid-2023 and implementing it (backed by technical standards) by late 2024 or 2025. Yet, the cross-cutting nature of the AI Act, coupled with the pervasive impact of AI, creates the risk of inconsistencies and overlaps with existing legislation, as well as possible conflicts with the substantive work being done at EU level on parallel related dossiers such as platform regulation, data governance and liability.

This study aims to contribute to the debate on the AI Act by helping EU institutions design a consistent regulatory framework and anticipate interactions with emerging and future initiatives (such as the European Health Data Space). We analyse the Commission proposal as complemented by the compromise texts of the Council under the Slovenian and French presidencies, as well as the myriad amendments submitted in the EP, to map possible inconsistencies with EU principles and rules, as well as potential loopholes and grey areas.

We draw on desk research and qualitative interviews conducted with leading AI experts from civil society, industry and academia, as well as an online workshop with experts on 23 June 2022. As a result, we identify several significant overlaps, gaps and inconsistencies between the proposed act and other EU rules, and highlight cases in which overall legal certainty and effective implementation and enforcement may be jeopardised.

More specifically, we map interactions between the proposed act and existing EU data protection law (the General Data Protection Regulation (GDPR), the 2016 Law Enforcement Directive (LED) and the reform of the ePrivacy Directive); the Cybersecurity Act; the provisionally agreed Digital Services Act (DSA) and Digital Markets Act (DMA); the new Data Governance Act (DGA); the recently launched Data Act; and the long-awaited Commission proposal on liability rules for AI systems. We also touch upon legislation that may appear more distant to EU digital policies, but remain nonetheless relevant when

addressing legal overlaps, gaps and inconsistencies with the AI Act, such as the reform of the Machinery Directive, the Trade Secrets Directive and the Unfair Commercial Practices Directive (UCPD).

The remainder of this study is structured as follows: Section 1 signals how the AI Act may appear far from a 'horizontal' piece of legislation. It summarises the main points of contention related to the overall scope of the act and the possible gaps it may create in terms of coverage of AI-related risks. Section 2 identifies a total of 35 legal overlaps, gaps and inconsistencies with other pieces of legislation. This part highlights possible unaddressed risks, as well as tensions and uncoordinated provisions in the domain of monitoring and enforcement of relevant EU law.

After a brief description of each issue, a comprehensive table distributes them across issue topics. In Section 3, this initial mapping is further broken down into eight key areas in which gaps and inconsistencies could create significant challenges.

The report concludes with a set of policy recommendations addressed to EU legislators, who are expected to formally adopt their respective policy positions over the coming months.

1. THE AI ACT: IS IT REALLY HORIZONTAL LEGISLATION?

The European Commission presented its proposal for an AI act in April 2021. In its explanatory memorandum (Section 1.1) it defined the act as a 'balanced and proportionate horizontal regulatory approach to AI', limited to the 'minimum necessary requirements to address the risks and problems linked to AI'. The proposal was originally grounded in a very broad general definition of AI (Article 3a), and included:

- an indication of the techniques considered to be covered by the definition (Annex I)[1];
- a rather parsimonious approach to regulation, based on the identification of a limited number of applications creating unacceptable risks to be prohibited altogether;
- a number of high-risk applications that, while not prohibited, should be subject to regulatory requirements;
- cases of moderate-risk AI for which transparency requirements would be needed.

In the words of the Commission, this approach, while casting a rather wide net on the possible applications that could be subject to regulation, ended up focusing on a tiny

[1] (a) Machine-learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning; (b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems; (c) Statistical approaches, Bayesian estimation, search and optimisation methods.

subset of AI products and services that are likely to enter the market in the coming years: a subset that was tentatively estimated by the Commission as corresponding to 5 to 10 % of the overall European AI market. When observed from this perspective, the original AI Act therefore appears far from over-regulatory, and potentially far from a 'horizontal' piece of legislation, at least when compared with existing legislation such as the GDPR.

Many features of the AI Act can lead *per se* to the emergence of gaps and possibilities to game the system. For example, the pre-identification of a limited number of high-risk AI applications in the proposed act shows implicit intent to leave out most of the solutions developed by large digital platforms in their consumer-facing AI deployment, ranging from content moderation to search engines and recommendation systems.

Rather than a willingness to avoid regulating these cases, the choice was motivated by the existence of a parallel stream of interventions, which culminated in the adoption of the EU digital services package, including the DSA and DMA. The resulting exclusion of certain applications from the list of high-risk AI, while aimed at avoiding costly redundancies and overlaps, may at the same time create gaps and inconsistencies.

This is especially the case if such uses are not subject to a similar set of provisions aimed at promoting trustworthy AI to those included in the scope of the AI Act. For example, the reference to third-party systemic risk assessment by very large online platforms (VLOPs) in the DSA bears no specific reference to the conformity assessment procedures envisaged in the AI Act, despite the fact that both aim to promote the protection of fundamental rights before AI solutions are deployed on the market, as well as post-market practices.

In summary, the decision to exclude certain applications from the concrete application of the AI Act may transform the envisaged task allocation between the DSA/DMA and the AI Act into a dangerous boundary between tectonic plates in the EU *acquis*: whether (to borrow from geologists' jargon) this ends up being a convergent, divergent or transform boundary, only time will tell. The substantial broadening of the list of high-risk AI proposed by the Council and the EP during the past months may frustrate the Commission's attempt to draw a precise frontier between the AI Act and other pieces of legislation. One example is the introduction of content moderation.

Another reason why the scope of the AI Act may be seen as under-comprehensive is the definition of risk that supports the pre-identification of AI applications subject to regulatory remedies. The act focuses on two main types of risks: those related to fundamental rights and those related to safety. This understanding of risks generated by AI may be seen as less than comprehensive, given that AI may potentially create risks and harms that go beyond these two categories, for example reaching wider societal and environmental dimensions, as well as epistemic considerations and psychological harms.

However, perhaps the most significant gap in the scope of the act relates to its specific, linear risk-based approach, inspired by a 'one AI system – one risk – one user' situation, rather than one in which several AI systems, regardless of their individual risk potential, end up interacting and generating significant risks for individuals and society as a whole. These so-called interactive risks of AI are so far excluded from the scope of the act and might be covered by the forthcoming EU legislative initiative on liability.

More generally, the horizontal nature of the act is limited by the various exceptions carved out by the Commission to sectoral legislation[2]. For instance, Article 2 of the proposal excludes systems used in the aviation, vehicle, marine and railroad sectors. This is justified in the proposal by the fact that current sectoral rules are already stricter than what this legislation would introduce. This is an issue since other heavily regulated domains fall under the scope of the AI Act. It could also create loopholes. For example, airport security (including crowd monitoring) may end up outside the scope of the AI Act, despite the latter's emphasis on safety and security risks.

Conversely, the proposal at times assumes that certain sector-related obligations are more far-reaching than they actually are. The opinion of the EP Committee on the Environment, Public Health and Food Safety (ENVI Committee) on the AI Act states that the proposal assumes that all AI applications used in the context of health are fully covered by Regulation (EU) 2017/745 governing medical devices. However, this regulation only covers medical devices and software with an intended medical purpose, and excludes health-related AI applications (such as those used to track medication) and administrative AI systems used by doctors in hospitals.

Among the other caveats of the legislation, AI systems used for military purposes, as well as third countries and international organisations acting in the framework of international agreements for law enforcement and judicial cooperation, are excluded from the scope of the AI Act.

This approach has been further reinforced through a recent Council compromise text agreed under the Slovenian presidency, which introduced an important exception for national security. This is problematic first because the notion of national security does not have a strict legal definition, but also because a maximalist approach could exclude a sizeable number of AI systems from the scope of the legislation.

These exemptions are forcefully opposed in the EP as they may create significant inconsistencies in the EU regulatory framework, given the inherent dual-use nature of many AI systems. Indeed, AI systems developed or used for military objectives could also

[2] Due to the vast number of policy sectors at stake, this study does not address the interplay of all sectoral legislation with the proposed act.

be used later for civil purposes, and many AI systems developed for civilian purposes can be employed by military and law enforcement.

Article 83 of the proposed AI Act also provides for various exceptions in the form of transition periods or even direct exclusions from the scope of the legislation. This is the case for AI systems used in the context of border control and security. These systems would only become subject to the rules of the AI Act if 'significant changes in the design or intended purpose of the system' are carried out after the adoption of the legislation. The implication is that certain practices prohibited by the AI Act would be allowed for border security as long as they were already implemented before the adoption of the law. This is true for any other high-risk AI systems under the scope of the act, including for instance online surveillance systems used for exams, which proliferated during the COVID-19 pandemic. These would not be subject to the new rules if already in place before the entry into force of the text.

Finally, similar considerations may hold for all those cases in which the risk generated by a given AI application depends on the interaction between more than one component assembled into a hardware-software system, featuring several (low risk) AI elements in one single product. The need to ensure the comprehensiveness of the AI Act suggests a fresh look at the AI value chain, as found in our companion paper. Authoritative scholars such as Stuart Russell have flagged the inconsistencies and perverse incentives that exclusive focus on deployed solutions may generate for entities involved in the whole value chain, for example at the pre-deployment stage[3].

In summary, even without looking at other existing or forthcoming pieces of legislation, the proposed act features a number of gaps, mostly caused by choices made in the definition of AI, in the risk classification system, in the definition of risk and in the focus on deployed applications. These gaps may become wider or narrower depending on the outcome of the negotiations between the co-legislators. For example, the compromise proposal of the Slovenian presidency contains a very narrow definition of AI, which may in turn lead to substantial gaps.

The corresponding proposal in the EP's IMCO-LIBE report is much broader and therefore less susceptible to this problem. Likewise, the notion of risk proposed by the IMCO-LIBE report significantly addresses risks to society and to the environment.

[3] See video at https://multimedia.europarl.europa.eu/en/webstreaming/event_20220321-1545-COMMITTEE-LIBE-IMCO?start=20220321145354&end=20220321175450 (minute 17:33).

2. IDENTIFYING OVERLAPS, GAPS AND INCONSISTENCIES WITH EMERGING EU *ACQUIS*

Beyond the specific features of the AI Act explored in the previous section, the proposal may also create overlaps, gaps and inconsistencies with the emerging EU *acquis* connected to this legislation, starting with existing EU data protection law.

This section comprehensively maps the gaps and limitations introduced by the proposal in relation to the fast-evolving field of EU digital policies. It draws on desk research and qualitative interviews conducted with leading AI experts from civil society, industry and academia, as well as an expert workshop organised online on 23 June 2022.

Overlaps, gaps and inconsistencies are mapped below with respect to seven policy domains: data protection (Section 2.1); the digital services package (Section 2.2); data governance (Section 2.3); cybersecurity (Section 2.4); unfair commercial practices (Section 2.5); intellectual property (Section 2.6); and liability rules (Section 2.7). Below, we illustrate outstanding issues that may require action by co-legislators in each of these areas.

2.1 THE EU DATA PROTECTION REGIME

2.1.1 The GDPR and the Law Enforcement Directive

The two main components of the current EU data protection framework, the GDPR and the LED, entered into force in 2018. Significant links can be found between these two pieces of legislation and the proposed act. Major gaps can be identified in relation to data processing, AI record keeping and privacy-enhancing techniques. Inconsistencies in the respective scope of the GDPR and the AI Act, as well as in what is considered high risk, illustrate the need to clarify the interplay between EU data protection *acquis* and the AI Act.

- *Data processing* (Data governance and management): Recital 41 of the proposal states that operators of AI systems must abide by the EU data protection regime, stating in particular that risk-based categories in the AI Act should not be interpreted as providing legal grounds for personal data processing. This provision lays the groundwork for compatibility between the AI Act and the GDPR, but its generality demands further specification of norms in both acts, as evidenced by the next sections.
- *Processing of special categories of personal data* (Data governance and management): Article 10 (paragraph 5) creates a legal basis for the processing of special categories of data under the AI Act. The interplay with the GDPR in this

context therefore appears incoherent with Recital 41, and the scope and conditions of this carve-out should be clarified. This issue could be addressed for instance by specifying more explicitly that Article 10 (paragraph 5) constitutes a proper legal exemption under the GDPR.

- *AI record-keeping* (Data governance and management): Article 12 AI Act states that '[h]igh-risk AI systems shall be designed and developed with capabilities enabling the automatic recording of events ("logs") while the high-risk AI systems [are] operating'. This obligation could lead to the systematic storage of personal data that AI systems may use. Article 12 fails to address its unclear connection with GDPR rules. Similarly, Article 61 AI Act introduces rules on post-market monitoring for compliance purposes, which could interfere with the data minimisation principle and strict data transfers mechanisms introduced in the GDPR. The process of obtaining consent from data subjects is unclear, as is the possibility to exercise their right to erase data.
- *Datasets and privacy-enhancing techniques* (Data governance and management): Article 25 GDPR on data protection by design and by default states that data controllers shall implement appropriate technical and organisational measures to protect the rights of data subjects and implement data protection principles, including data minimisation. This may conflict with Article 10 AI Act indicating that training, validation and testing datasets of high-risk AI systems shall be relevant, representative, free of errors and complete. Article 10 AI Act could take better into account the obligation of privacy-enhancing techniques under GDPR rules, especially in the context of high-risk AI systems. These techniques may involve, for instance, the increasing use of synthetic data. This would allow AI providers to stay in line with the protection by default requirement in Article 25 GDPR, but could inevitably fail to render the data 'free of errors'.
- *Biometric identification* (Data governance and management): While the LED offers a comprehensive framework to allow European law enforcement authorities (LEAs) to collect and process data for law enforcement purposes, the AI Act can be considered as *lex specialis* to this directive, as it would ban real-time biometric identification with certain (substantial) caveats. While it could be argued, for instance, that real-time facial recognition should in theory be forbidden on the grounds of the LED, the AI Act may inadvertently legalise certain AI-driven systems through the various exceptions envisioned both in the Commission proposal and in the Council compromise texts.

  Indeed, the current Commission proposal only bans a narrow set of practices while categorising others as high risk, thus conflicting with the EU data protection *acquis*. In addition, several Members of the European Parliament (MEPs), on behalf of the Greens / European Free Alliance (EFA), have proposed to further extend the scope of biometric data processing included in the AI Act by introducing the broader notion

of 'biometrics-based data'. This would cover situations where the data in question may not confirm the unique identity of an individual as understood in the GDPR.

- *Emotion recognition* (Data governance and management): Biometric identification refers to identifying who someone is based on biometrics (face, voice and fingerprints), whereas emotion recognition is about identifying a person's inner emotional state based on their face, tone of voice, body movement or words spoken (this is also called affective computing). The AI Act does not prohibit systems capable of recognising emotions. Emotion recognition AI systems are now assigned to the 'limited risk' category, despite often being considered a high-risk practice under the GDPR, since this application of AI implies many risk factors drawn out by the European Data Protection Board (EDPB) for consideration when determining the level of risk and the need for a data protection impact assessment (DPIA). A recent brief by Access Now indeed suggests that emotion recognition technologies can significantly undermine one's right to privacy. There is therefore a need to align the provisions of the AI Act with the GDPR in relation to emotion recognition technologies.

- *Dark patterns* (Data governance and management): Dark patterns are a GDPR issue under its Article 25. Recently, the EDPB proposed a set of recommendations aimed at tackling dark patterns, while at the same time acknowledging that not all dark patterns lead to a GDPR infringement. Dark patterns are also regulated in the agreed version of the DSA, which includes in its Recital 51b and Article 23a a qualified ban on dark patterns on the interfaces of online platforms. More specifically, the DSA states that 'providers of intermediary services should therefore be prohibited from deceiving or nudging recipients of the service and from distorting or impairing the autonomy, decision making, or choice of the recipients of the service via the structure, design or functionalities of an online interface or a part thereof'.

  The DSA also indicates that the Commission may issue guidance on the application of this prohibition to specific practices. Finally, dark patterns are partially covered by the UCPD. In the AI Act, dark patterns fall within the scope of the ban of subliminal use of AI (Article 5). As such, they could be considered to be in the 'unacceptable risk' category. These myriad legislative and non-legislative rules addressing dark patterns generate limited clarity on their joint implementation. The regulatory approach deriving from the UCPD, DSA, AI Act norms and GDPR implementation text could be clarified in the upcoming Commission guidance on the matter.

- *AI-system user* (Definitions): The lack of alignment in the terminology used in the GDPR and AI Act could become a major challenge in ensuring compliance. In the GDPR, the term 'user' refers to the data subject, while in the AI Act the notion of

'user' corresponds to the user of an AI system, which could be a data controller according to the GDPR definition.

- *Research purpose* (Definitions): Unlike Article 89 GDPR, which provides for exceptions to data protection rules for research purposes, the AI Act does not offer a comparable exemption for scientific projects, which may run the risk of being subject to the same obligations as AI providers when publishing their AI models in academic settings. The AI Act could, for instance, clarify that publishing models and putting them online to access for free (making them open source) would not constitute putting them on the market (thus not triggering the requirements).
- *Public and private data controllers* (Definitions): Several provisions of the AI Act (for instance in relation to the real-time processing of biometric data or social scoring) create a distinction between public and private actors in relation to their obligations. There is therefore an inconsistency with the general approach of the GDPR, which does not differentiate data controllers on this basis.
- *AI with high risk* (Risk-based approach): Article 35 GDPR contains rules for performing a DPIA, and its paragraph 3 underlines the cases in which a DPIA is required. It should therefore be clarified whether the categorisation of AI systems as high risk would, by default, categorise them as high risk on the grounds of the GDPR, and with which legal consequences.
- *AI-driven manipulation* (Risk-based approach): Though the GDPR covers the automated tracking and processing of data through AI systems, it only does so when this leads to individual forms of profiling. The individualistic approach of the GDPR fails to cover AI-driven manipulation that could have a collective effect on segments of society, rather than individual impacts. The current proposal does not address this gap, but could do so via a larger ban on certain techniques allowing such manipulation.
- *CE marking of conformity* (Liabilities): Article 49 AI Act on CE marking of conformity does not take into consideration the codes of conduct and certification mechanisms from Chapter 4 GDPR in relation to data protection as criteria for the issuance of CE marking by notified bodies. When subject to other EU legislation that also provides for CE marking, greater alignment could be ensured by indicating whether the AI system also fulfils the requirements of the other legislation (for instance in the case of the health sector). The general rule is that any provider needs to 'make sure that its product complies with all the relevant requirements before affixing the CE marking to it'.

- *Compliance and impact assessment* (Enforcement): The AI Act does not provide for some form of ex ante assessment of compliance with fundamental rights, except for high-risk systems. As a result, the AI Act goes against the rules of the GDPR, according to which certain machine-learning processing of personal data requires a DPIA. Indeed, as well evidenced by a recent European Parliamentary Research Service (EPRS) study, a DPIA is required in the case of 'processing on a large scale of special categories of data', but also the 'systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person'. Requiring high-risk AI system users to conduct an AI impact assessment similar to those in Article 35 GDPR could be a possibility. The actors responsible for this assessment would need to be better harmonised, as the proposal currently requires the system provider to carry out the risk assessment, while in the GDPR it is the user who performs the role of data controller and carries out the risk assessment.

2.1.2 The ePrivacy Directive and its reform

Started in 2017, the reform of the ePrivacy Directive into a new regulation has been and remains a very controversial process. While limited progress has been observed in accommodating the conflicting positions of the Council and the EP in trilogues over recent months, this process is important to follow in light of the AI Act, notably given its implications for the privacy of electronic communications. Indeed, the possibility that the scope of the ePrivacy Regulation will include machine-to-machine (M2M) data processing or restrict the capacity of AI providers to train AI systems is a potential area of concern.

- *M2M data processing* (Data governance and management): While supporting the development and deployment of AI systems, the AI Act fails to consider the necessary regulatory steps needed to allow greater legal certainty in relation to M2M data processing. As already shown by Storms, Valcke and Kindt (2019), M2M communication is not clearly considered as protected communication in the ePrivacy Directive. In the context of the long-awaited reform of the ePrivacy Directive, there is a need to ensure that M2M data processing does not fall within the scope of the electronic communications covered by the future ePrivacy Regulation.
- *Training of AI systems* (Data governance and management): Article 10 AI Act should be changed so that the ePrivacy Regulation institution of 'compatible purpose' may be applied explicitly to the training purpose of AI systems. In this case, it is doubtful whether consent should be used as a form of privacy protection mechanism.

2.2 THE EU DIGITAL SERVICES PACKAGE

2.2.1 The Digital Services Act

To be formally adopted by the EP and the Council in summer 2022, the new DSA creates a few requirements in relation to recommender systems and algorithmic accountability that should be better recognised in the AI Act.

- *Recommender systems* (Risk-based approach): Recommender systems fall within the scope of both the DSA and AI Act proposals. Yet, they approach recommender systems in two distinct ways. The DSA looks at recommender systems implemented by VLOPs and very large online search engines, while the AI Act focuses mainly on a narrow subset of high-risk systems. Currently, few recommender systems used by VLOPs will also qualify as high-risk AI systems, so most will be bound by either the rules of the AI Act or the DSA, but not both. However, there are some clear examples that will fall under both laws, such as recommender systems on VLOPS for advertising job vacancies (high risk under Annex III to the AI Act); in this case, the DSA's requirement that there must be an option for a recommender system not based on profiling (Article 29 DSA) and the AI Act's requirement for accuracy and robustness (Article 15 AI Act). Proposed changes to the high-risk categories of the AI Act, such as the inclusion of AI systems that interact with children, could substantially expand the number of overlapping systems.
- *Researchers' data access* (Data governance and management): One of the changes brought by the DSA proposal is the introduction of the possibility for vetted researchers to access the data of VLOPs to understand how their algorithms function and what their implications are in relation to online risks. The fact that the DSA provides for the potential for auditing and oversight of the high-risk AI systems built into VLOPs is currently not recognised in the AI Act.

2.2.2 The Digital Markets Act

Now provisionally agreed, the new DMA introduces a new competition framework for the digital economy, including new obligations for so-called gatekeepers. These obligations refer, for instance, to the sharing of datasets, intersecting with the AI Act. However, the DMA fails to introduce specific measures for the increasingly concentrating market of AI providers.

- *Gatekeepers and datasets* (Data governance and management): The AI Act and DMA should use harmonised definitions for gatekeepers in relation to datasets. This would be needed to thoroughly understand where to draw the line when deciding which datasets should be siloed between services, leveraged across the platform, or shared externally. With the DMA (Article 5), gatekeepers are indeed banned from combining

'personal data from the relevant core platform service with personal data from other core platform services or from any other services provided by the gatekeeper or with personal data from third-party services' and 'cross-use personal data from the relevant core platform service in other services provided separately by the gatekeeper, including other core platform services, and vice-versa'. At the same time, Article 6 (10) DMA states that:

> the gatekeeper shall provide business users and third parties authorised by a business user, at their request, free of charge, with effective, high-quality, continuous and real-time access to, and use of, aggregated and non-aggregated data, including personal data, that is provided for or generated in the context of the use of the relevant core platform services or services provided together with, or in support of, the relevant core platform services by those business users and the end users engaging with the products or services provided by those business users.

As stated by Lindholm (in Bertuzzi, 2022), these new obligations will make it 'difficult for the gatekeepers to thoroughly understand where to draw the line between personal data and anonymous data when trying to figure out what data sets should be siloed between services and which data sets could actually be leveraged across the platform'. This has a direct implication for the AI Act, notably in relation to access to training, validation and testing datasets, but also for the development of datasets for AI systems by gatekeepers. The main issue resides in the fact that the DMA and the AI Act fail to harmonise the definitions of the notions of databases and datasets, which may introduce inconsistencies for gatekeepers.

- *AI innovation and competition* (Enforcement): The development stage of the AI Act calls for specific consideration of potential competition issues in the field of AI. As argued in a recent report by Codagnone, Liva and Rodríguez de las Heras Ballell (2022), EU legislators need to 'better address the risks of new emerging monopolies without compromising innovation'. The rules of the DMA alone do not provide for AI-specific provisions, signalling a potential gap in the regulatory framework.

2.3 EMERGING EU DATA GOVERNANCE RULES

2.3.1 The Data Governance Act

Provisionally agreed by the EP and the Council in spring 2022, the DGA is an important step in the implementation of the 2020 European data strategy. The data-sharing frameworks and the enforcement mechanism introduced by this legislation have implications for the AI Act.

- *Data-sharing frameworks* (Data governance and management): Presented as a piece of legislation designed to unlock the potential of AI by facilitating data sharing, the DGA raises a number of issues regarding its interplay with the AI Act. Indeed, certain provisions of the DGA (Article 9 in particular) will create new obligations for data-sharing intermediaries and may restrict their ability to deploy AI systems.
- *European Data Innovation Board* (Enforcement): The enforcement mechanism in the Data Act proposal (see below) does not achieve sufficient synergies with those envisioned in other directly relevant legislation such as the DGA and the AI Act. The European Data Innovation Board created by the DGA could be better leveraged in the context of the AI Act and Data Act to ensure more meaningful and efficient coordination between competent national authorities, as suggested by Prufer and Graef (2021).

2.3.2 The Data Act and the Database Directive

On 23 February 2022, the European Commission published its long-awaited legislative proposal for a new Data Act. It aims to challenge the constitution of data monopolies across various sectors by reshaping existing power structures that favour large data incumbents and moving to solidify data as a non-rival good.

This legislation also includes a provision that the sui generis database right from the Database Directive[4] 'does not apply to databases containing data obtained from or generated by the use of a connected device'. Both texts have implications for the AI Act, first in light of the new requirements for data transfers proposed under the Data Act, but also in relation to the protection of datasets.

- *Cloud computing and data transfers* (Data governance): The regulatory approach of the Data Act, namely to enhance data sharing while creating new legal constraints for cloud providers, may lead to some interferences with the goals of the AI Act. As AI systems rely heavily on cloud computing power, the new proposed rules, such as Article 27 of the Data Act on international transfers (below) could become detrimental to the uptake of AI systems in the EU:

> Providers of data processing services shall take all reasonable technical, legal and organisational measures, including contractual arrangements, in order to prevent international transfer or governmental access to non-personal data held in the Union where such transfer or access would create a conflict with Union law or the national law of the relevant Member State.

[4] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases.

- *Datasets protection* (Data governance): Article 3 of the Database Directive provides that datasets can be protected by trade secret according to intellectual property rights (IPR) when they are original. The need to reuse datasets and data sharing, as envisioned in the AI Act, appears to be in contradiction with the Database Directive. The application of the so-called sui generis database right to Internet of Things and machine-generated data is unclear. As suggested by legal scholars, there is a need to amend the Database Directive to reduce IPR over datasets.

2.4 CYBERSECURITY

Adopted in 2019, the Cybersecurity Act is one of the core pillars of the EU cybersecurity *acquis*. Provisions regarding the security and certification of AI systems in the AI Act appear inconsistent with the mechanisms introduced by the Cybersecurity Act.

- *Security certification* (Liabilities): The AI Act aims to further improve the security of AI systems via a certification process that is not entirely consistent with the certification process introduced by the Cybersecurity Act. As argued by Casarosa (2022), 'although the AI Act hints at a possible path towards mutual recognition of certifications, a deeper analysis of the provisions and a comparison between the underlying features of the certification mechanisms show that the different approaches adopted in the two acts may undermine the goal of certification mechanisms as trust-enhancing and transparency instruments'. This inconsistency, which can also be observed with the GDPR certification process, needs to be addressed to ensure greater compliance.

2.5 RULES ON LIABILITY

2.5.1 The Machinery Directive and its reform

Launched in 2021, the process of revising the Machinery Directive into a regulation[5] aims to revamp the existing regulatory framework for placing machinery on the single market. The Commission proposal recognises the need to address the implications of advanced robots and new digital technologies such as AI for product safety, and its Recital 19 states the need to avoid incoherencies between the upcoming Machinery Regulation and the AI Act. Yet, certain issues deserve closer attention regarding both definition and conformity assessment.

- *Substantial modifications* (Definition): The definition of 'substantial modifications' should be made explicit in the AI Act. The proposal for a Machinery Regulation

[5] Proposal for a regulation of the European Parliament and of the Council on machinery products.

introduces explicit reference to modifications of products already placed on the market or into service.

- *High-risk machinery* (Definition): Recital 45 of the proposed Machinery Regulation states that 'software ensuring safety functions of machinery based on artificial intelligence, embedded or not in the machinery product, should be classified as a high-risk machinery product due to the characteristics of artificial intelligence such as data dependency, opacity, autonomy and connectivity, which might increase very much the probability and severity of harm and seriously affect the safety of the machinery product'. The distinction between high-risk AI systems under the AI Act and high-risk machinery with an AI component should be made clearer considering the distinct obligations and requirements that both categories need to comply with.
- *Conformity assessment* (Enforcement): Conformity assessment provisions in Article 22 of the Machinery Regulation should be aligned with Article 41 AI Act, and should consider the need for multiple assessment attempts after the product is put on the EU market, as well as new CE marking.
- *Safety requirements* (Liabilities): While the draft regulation currently adopts the same definition of AI, the AI Act and the Machine Regulation could eventually provide diverging definitions or safety requirements for the same product. In this instance, it is unclear which would be given precedence.

2.5.2 Proposal on liability for AI

I European Commission is expected to release a new legislative proposal in 2022 to reform the liability regime for AI systems. The interplay between this forthcoming proposal and the AI Act is significant, though limited insights are currently available on the future shape of the proposal. Two main points can already be identified though in relation to strict liability rules for high-risk AI systems and the reporting of incidents.

- *Strict liability for high risk* (Liabilities): Article 6 AI Act on the high-risk category appears inconsistent with the existing *acquis* in relation to liability rules. The liability regime in case of damages caused by AI systems is due to evolve with the upcoming Commission proposal to be released in 2022. Until then, it is unclear whether the designation of high risk should lead to the application of strict liability rules, as it does for other sectors. In 2020, the EP suggested introducing a risk-liability regime for AI systems to strengthen the connection between the upcoming proposal and the AI Act.
- *Reporting of incidents* (Liabilities): Article 62 AI Act on the reporting of serious incidents and of malfunctioning introduces an obligation for AI providers to report incidents when a causal link has been established between the AI system and the

incident. The question then arises whether such notification of a causal link can be sufficient for the purpose of establishing liability.

2.6 EU PROVISIONS ON UNFAIR COMMERCIAL PRACTICES

2.6.1 Unfair Commercial Practices Directive

Adopted in 2005 and amended in 2019, the UCPD is an important pillar of the EU *acquis* in the field of consumer protection. The AI Act aims to address several loopholes or gaps in the UCPD that already prohibit unfair commercial practices leading to economic or financial harm to consumers.

- *The notion of harm* (Definitions): In the AI Act, the Commission proposes narrowing the scope of the harm requirement in Article 5, understood as 'physical and psychological harm'. This approach creates a few challenges, however, highlighted by Georgieva, Timan and Hoekstra (2022). Indeed, 'as known from tort liability law, to demonstrate or prove individual harm even when the latter is probable is nearly impossible, though the proof will be required by Article 71(3)(a) AI Act to impose a fine'. In addition, the approach taken by the Commission appears to limit the possibility for collective harms.

2.6.2 The Platform-to-Business Regulation

Adopted in 2019, the Regulation on fairness and transparency for business users of online intermediation services, known as the Platform-to-Business Regulation (P2B Regulation), could be better aligned with the AI Act. Indeed, its provision on algorithm disclosure appears not to be fully aligned with the transparency requirements envisioned in the AI Act.

- *Algorithm disclosure* (Liabilities): Recital 27 P2B Regulation states that 'providers of online intermediation services or of online search engines should not be required to disclose the detailed functioning of their ranking mechanisms, including algorithms, under this Regulation'. As a result, the AI Act should refine the interplay between the two texts to avoid inconsistencies in relation to the disclosure of algorithms.

2.7 INTELLECTUAL PROPERTY: THE TRADE SECRETS DIRECTIVE

The Commission proposal on the AI Act requests that information on the development and performance of high-risk AI systems is shared by several actors to verify their compliance. The information requested includes the general characteristics, capabilities and limitations of the systems, algorithms, data, training, testing and validation processes, and documentation on the relevant risk-management systems. This inevitably intersects with the Trade Secrets Directive.

- *Protection of trade secrets* (Data governance and management): Several MEPs, including Axel Voss and Eva Maydell, have highlighted the need to preserve trade secrets in the AI Act. It is indeed unclear whether the logs that are generated automatically by high-risk AI constitute trade secrets, and whether they should be treated as such by national authorities. This would require keeping such information confidential and secured, suggesting an indirect obligation for Member States to provide their national supervisory authority with the necessary resources in terms of cybersecurity, which they may currently lack.
- *Sandboxes* (Data governance and management): The Commission proposal does not provide a legal basis for the use of data protected by trade secrets to develop certain AI systems in the public interest within the AI regulatory sandbox. This addition would be needed to limit liability risks during experimentation in the AI sandbox.

2.8 SYNOPTIC TABLE

To conclude this section, the following table summarises the state of play of current policy debates around the key dimensions of the AI Act. These categories, or baskets, provide a suitable analytical framework to explore the interplay between the AI Act's current draft texts with other (forthcoming) EU legislation.

Table 1: Synopsis of issues under study

	Definitions/Scope	*Risk-based approach*	*Data governance*	*Liabilities*	*Enforcement*
GDPR and LEA Directive	Research purpose Public and private data controllers AI systems user	AI with high risk AI-driven manipulation	Data processing Processing of special categories of personal data AI record keeping Datasets and privacy-enhancing techniques Biometric identification Emotion recognition Dark patterns	CE Marking of conformity	Compliance and impact assessment
ePrivacy Directive and Regulation			M2M data processing Training of AI systems		
Digital Services Act		Recommender systems	Researchers' data access		
Digital Markets Act			Gatekeepers and datasets		AI innovation and competition
Data Governance Act		Data-sharing frameworks			European Data Innovation Board
Cybersecurity Act				Security certification	
Data Act and Database Directive			Cloud computing and data transfers Protection of datasets		
Machinery Directive and Regulation	Substantial modifications High-risk machinery			Safety requirements	Conformity assessment
P2B Regulation				Algorithms disclosure	
Proposal on liability for AI				Liability for high-risk Reporting of incidents	
Unfair Commercial Practices Directive	Notion of harm				
Trade Secrets Directive			Protection of trade secrets Sandboxes		

3. POLICY RECOMMENDATIONS: ADDRESSING THE INTERPLAY BETWEEN THE AI ACT AND EU *ACQUIS*

The first sections of this report identified several gaps, inconsistencies and overlaps created by the proposed AI Act with respect to the EU digital *acquis*. Below, we provide policy recommendations for a select number of challenges identified as particularly important. These will ensure that implementation of the AI Act can occur without significant shortcomings with respect to regulatory certainty, avoidable regulatory costs or possible incentives to circumvent legal provisions.

3.1 CLARIFY AND ALIGN TERMINOLOGY WITH EXISTING EU LEGISLATION

At the core of the proposal, **the definition of what is considered an AI system is expectedly subject to significant controversies**. A broad definition might entail that the legislation affects most software or algorithms circulating in the EU single market[6], even if the risk-based approach adopted by the AI Act and the introduction of Annex I potentially mitigate the risk.

On the other hand, adopting a narrow definition may imply that the regulatory requirements, notably in terms of transparency and liabilities for AI providers, only apply to a subset of AI systems. This, in turn, may lead to the incentive to choose suboptimal solutions by relying on certain techniques, simply because they are not covered by the regulatory framework. Moreover, focusing on techniques rather than approaches might incentivise AI developers to define their techniques in ways that evade the scope of the legislation.

This has led some experts to call for the reintroduction of the definition of AI developed by the Commission's High-Level Expert Group on AI, which refers to the characteristics of AI rather than the technology itself, or of the internationally agreed Organisation for Economic Co-operation and Development definition (as advocated by the opinion of the Committee on Industry, Research and Energy (ITRE) in the EP[7]).

[6] In this regard, the definition of a general-purpose AI system is subject to several conflicting interpretations, and requires additional explanation and discussion. This and related issues are further explored in the context of a forthcoming companion study.

[7] The opinion of the ITRE Committee states that 'the notion of AI system should be clearly defined to ensure legal certainty, while providing the flexibility to accommodate future technological developments. This definition should be in line with definitions that have been accepted internationally. The definition should be based on the key functional characteristics of the AI system, in particular the ability, for a given set of human-defined objectives, to make predictions, recommendations, or decisions influencing real or virtual environments'.

The **AI Act should thus make clear whether it is expected to apply to all algorithms or to a certain range of machine-learning systems**. The current uncertainty risks creating significant points of friction in light of existing legislation already governing more traditional software.

Furthermore, with respect to defining the actors and organisations that participate in the so-called AI lifecycle, several important issues should be highlighted. First, **the definition of the term 'AI lifecycle' is not made clear in the Commission proposal**. Although the key actors within the value chain are defined, a comprehensive definition is not provided. Also, actors deploying AI systems developed by others are qualified in the proposal as 'users'. This term could be confusing, as echoed by a recent report of the Ada Lovelace Institute that suggested referring instead to the notion of 'deployer'. This would be in line with the language used in many other reports, including the 2021 study by Renda et al. that backed the impact assessment of the AI Act.

Several MEPs have supported this proposal, as shown by the amendments submitted in the EP. Moreover, instead of the generic notion of 'provider', the Renew Europe group in the EP supports the use of the term 'developer', suggesting it would be more accurate and is already more widely used.

In addition, **the notion of end recipient is currently absent from the Commission proposal**. As advocated by various civil society organisations and the opinion of the ENVI Committee, 'many of the applications mentioned in the proposed AI Act will involve not just users but end recipients', which thus calls for the introduction of a new definition of end recipient[8], granting them the appropriate degree of transparency and provision of specific information.

Finally, the Commission proposal refers to the notion of small-scale provider, as opposed to the more traditional notion of SME, as defined by Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises. As shown by various EP amendments, opting for the notion of SME would create more legal certainty for companies.

[8] The opinion of the ENVI Committee proposes the following definition: 'end recipient' means any natural or legal person, other than an operator, to whom the output of an AI system is intended or to whom that output is provided.

01 The definition of what is considered an AI system in the AI Act, as well as the actors and organisations that participate in the so-called AI lifecycle, needs to be made clearer. Greater alignment with internationally agreed definitions and existing terminology in the EU digital policy *acquis* should be guaranteed to ensure consistency.

3.2 ADDRESS INTERACTION WITH SECTOR-SPECIFIC LEGISLATION

As highlighted by the Ethics guidelines for trustworthy AI (2019) developed by the Commission's High-Level Expert Group on AI, 'besides horizontally applicable rules, various domain-specific rules exist that apply to particular AI applications'. This is the reason why the AI Act would benefit from additional fine-tuning with sector-specific legislation.

In relation to **health**, the limited alignment between health-related rules and the proposed AI Act needs to be addressed. This has led the Greens/EFA group to advocate for certain AI systems used in the area of healthcare, but not covered by the Regulation on Medical Devices, to be considered as high risk in the AI Act. This proposal is justified by the fact that software impacting diagnostics, treatments or medical prescriptions and access to health insurance can significantly affect health and safety.

The proposed act could also further clarify the scope of certain sectoral exemptions, especially for broad sectors **such as aviation, vehicle, marine and railways**, which were originally excluded from the proposal.

In relation to the proposed **exception for national security and military systems**, greater coherence between the recently approved Regulation on Dual-use Items and the AI Act would be welcome. A possibility could be to add a provision to the AI Act stating that it shall apply to AI systems developed or used as dual-use items.

02 The AI Act requires additional fine-tuning with sector-specific legislation. Carve-outs for specific sectors currently create unintended loopholes, for example in relation to the health sector. This also applies to military and security applications, creating a need for the AI Act to clearly state that it applies to AI systems developed or used as dual-use items.

3.3 REFINE COMPATIBILITY WITH DATA PROTECTION AND GOVERNANCE RULES

While the proposal states that operators of AI systems must abide by the EU data protection regime, suggesting strong compatibility between the AI Act and the GDPR, many provisions of the proposed legislation pose significant challenges for the enforcement of existing EU data protection rules.

These conflicting goals and policy objectives stem from the different legal bases of the legislation (data protection or market harmonisation, under Articles 16 and 114 respectively of the Treaty on the Functioning of the European Union), but also because they originate from separate policy processes. For instance, a recent CEPS report illustrates how the new EU Data Act proposal signals a significant shift in the EU's approach to the wider data economy, from championing the free flow of non-personal data in the context of the 2016 digital single market (DSM) strategy to the introduction of specific requirements for governing and limiting data transfers in the context of the Data Act under the Von der Leyen Commission.

The AI Act's formulation process is deeply shaped by this tension between proponents of increased data sharing and access, and other more privacy-oriented approaches, which as a result generate a certain **confusion in the main provisions regarding data governance and management**.

More fundamentally, one of the stated aims of the AI Act is to increase the uptake of AI systems at EU level, which themselves require access to large amounts of data and intensive data-processing capabilities, but also wider access to training datasets. Inevitably, this objective enters into **conflict with other principles embedded in EU data protection law, such as data minimisation or data protection by default**.

This had led several MEPs, including the co-rapporteur Brando Benifei, to suggest new wording for Recital 2, stating 'this Regulation should not affect the restrictions, prohibitions or enforcement that apply where an artificial intelligence practice infringes another EU law, including EU *acquis* on data protection, privacy, or the confidentiality of communications'.

A case in point is the current **uncertainty regarding the compatibility of the AI Act with the GDPR in relation to the datasets required to train, validate and test them**. It remains unclear whether the processing of personal data needed to meet the transparency requirements of the AI Act could be considered as lawful under the GDPR.

This is the reason why several MEPs advocate that such processing should be considered as lawful for the purpose of the legitimate interest of the provider under the GDPR, while others use this ground to criticise the obligation to automatically record events when

high-risk AI systems are operating. Other examples include the uncertainty related to the interplay of the AI Act with Article 22 GDPR on automated data processing, or the perimeter of the legal basis introduced in Article 10 AI Act for the processing of special categories of personal data.

New rules governing data flows, including the proposed Data Act and ePrivacy Regulation, suggest other potential interferences with the AI Act's ambition to enhance the uptake of AI systems in the EU, taking the form of new legal constraints for cloud providers for instance.

03

The AI Act proposal has generated a degree of confusion in relation to the governance of data and its compliance with GDPR rules. It should be clarified whether the processing of personal data needed to meet the transparency requirements of the AI Act, notably in relation to training datasets and automatic logs for high-risk AI systems, could be considered as lawful under the GDPR.

3.4 STRENGTHEN THE AI ACT'S RISK-BASED APPROACH

The AI Act explicitly follows a risk-based approach. However, **the criteria for an AI system to be considered as posing unacceptable risks are unclear**. For example, the inclusion of systems that manipulate people through subliminal techniques appears intuitive, but in practice it is unclear what the threshold is for the manipulation becoming so significant that the application crosses the line. This threshold may have to be clarified through future interpretive guidance, also in relation to the scope of existing provisions such as the GDPR and consumer protection legislation.

A **similar set of considerations applies to the definition of high-risk applications**, for which the list and criteria proposed in the text have been subject to lively debate, **also given that the list** (originally described by the Commission as potentially referring to a small subset of future AI systems on the market, e.g. 5 to 10 %) **keeps expanding**. his is well illustrated by a recent proposal in the draft report of two EP committees[9] to qualify as 'high risk' any AI systems used in insurance and medical triage, as well as AI systems that interact with children or affect democratic processes.

[9] Committee on Internal Market and Consumer Protection (IMCO) and Committee on Civil Liberties, Justice and Home Affairs (LIBE).

In the Commission proposal, **most of the transparency measures** envisioned for high-risk AI systems – notably in relation to their registration in the EU-wide high-risk AI systems database – **apply to the deployers of these systems, not to the actors developing them**. A recent Mozilla report argues that 'deployers must therefore be obligated to disclose AI systems they use for high-risk use cases and provide meaningful information on the exact purpose for which these high—risk AI systems are used as well as the context of deployment'.

Finally, Recital 41 on high-risk classification suggests that all AI systems in this category should be considered as lawful under national or European laws, and thus tends to frame the AI Act as a minimum harmonisation rule. This aspect should be further clarified, however, given its implications for the interplay between the AI Act and national and European laws.

04 In the AI Act, the criteria for an AI system to be considered as posing unacceptable risks are not clearly laid down. The threshold should be clarified through future guidance, also in relation to the scope of existing provisions such as the GDPR and consumer protection legislation.

3.5 BETTER INTEGRATE THE AI ACT WITH EU PRODUCT SAFETY RULES

Regarding liability and product safety, the AI Act draws on the regulatory framework of the New Legislative Framework (NLF) designed to ensure the safety of products in the EU market. As described by Veale and Zuiderveen Borgesius (2021), 'under NLF regimes, a manufacturer must undertake pre-marketing controls undertaken to establish products' safety and performance, through conformity assessment to certain essential requirements laid out in law. Manufacturers then mark conforming products with "CE"; marked products enjoy EU freedom of movement'.

The question remains whether this is the most relevant approach to a non-tangible product such as an AI system, and **whether it should apply to standalone AI systems as much as to AI systems built into products covered by the NLF**.

Existing EU product safety rules have been formulated for traditional manufacturing models, but far less so when the manufacturers are so-called AI providers. Indeed, traditional manufacturers are usually directly responsible for making sure that a product is safe, and thus face the most obligations.

However, **the very nature of AI systems can make it difficult for AI providers to make their 'products' safe**, first because AI systems are not necessarily static, but also because they are not always produced, transformed and used by only one organisation. This will be described in more detail in our forthcoming companion study on the AI value chain.

The **AI Act should ideally address the distribution of responsibilities between providers and deployers, bearing in mind the context and environment, throughout the AI lifecycle.** Though an upcoming Commission proposal to be released in 2022 is expected to propose new liability rules for the AI sector, the AI Act already needs to be consistent with the existing *acquis* in relation to liability rules (for instance the Product Liability Directive or the Use of Work Equipment Directive).

05 The NLF should recognise the specificities of non-tangible products such as AI systems. In line with existing and forthcoming liability rules, the AI Act needs to better address the distribution of responsibilities between providers and deployers, bearing in mind the context and environment, throughout the AI lifecycle.

3.6 ESTABLISH A STRONGER ECOSYSTEM OF ENFORCEMENT

The AI Act has been criticised for its limitations in terms of enforcement. This can be explained by the very nature of the enforcement instruments envisioned in the act, as well as the current lack of an 'ecosystem of oversight' (De Streel and Ledger, 2021) and the diverging enforcement mechanisms of new digital-related legislation (such as the DGA, Data Act and DSA/DMA). **A unified enforcement agency would have the potential to exploit synergies and economies of scope and scale in enforcement, at the same time reducing the administrative burden and compliance costs for regulated entities**. This, in turn, would also boost the effectiveness of EU law enforcement.

The post-market enforcement processes of the AI Act have been repeatedly described as weak. Market surveillance authorities – the national authorities that would be primarily responsible for the enforcement of the rules – are known for being less active than data protection authorities (DPAs). This challenge is further amplified by the fact that **the proposed EU AI Board currently has limited purpose or power**.

The EP and the Council are in the process of formulating their preferred approach towards the ecosystem of enforcement, in parallel with beginning negotiations on the Data Act. Several actors, for instance the Greens/EFA group in the EP, support the idea that the competent authority under the AI Act should be the supervisory authority

established under the GDPR, to avoid duplication and combine expertise and competences.

At Member State level, national DPAs are already set to enforce the GDPR, the EU Data Protection Regulation (EUDPR) and the LED regarding AI systems involving the use of personal data. Hence, **the designation of DPAs as national authorities pursuant to Article 59 AI Act would seem appropriate due to the significant overlap of scope of competences and work under the AI Act and EUDPR**, as already suggested by the joint opinion of the EDPB and European Data Protection Supervisor (EDPS) on the AI Act.

The French presidency of the Council has argued instead in favour of removing the notion of supervisory authority at national level, 'giving Member States more flexibility in the designation of the entities responsible for the coordination and implementation of the AI Act'.

Alternatively, other MEPs advocate for the creation of an AI Advisory Council to support the work of the EU AI Board. This Board would be renamed the European Union Artificial Intelligence Office under the proposal of EP co-rapporteur Dragoş Tudorache.

Drawing on the challenges faced in the implementation of the GDPR, and as already suggested by the policy direction taken in the DMA, several voices now support transferring stronger enforcement powers to the European Commission than initially envisioned, **especially when national market surveillance authorities have not taken measures against infringement**.

In addition, Chapter III AI Act poses specific challenges in terms of enforcement. **For most high-risk AI systems, requirements can be met with self-certification processes only**. The challenges posed by the enforcement of data protection rules vis-à-vis large tech players suggest that *ex ante* third-party certification would be a more powerful option, though potentially burdensome for many AI providers and deployers (even if the extent of this burden would depend on the percentage of AI systems classified as high risk).

Finally, the AI Act does not provide sufficient rights to citizens to make complaints about AI systems, either individually or collectively. To remedy the lack of collective redress mechanisms, a proposal supported by the consumer organisation BEUC would consist of adding the AI Act to the Annex to Directive 2020/1828/EC on Representative Actions for the Protection of the Collective Interests of Consumers, 'which lists the laws where it is possible to file a representative action', so that **it would become possible to file collective redress in the case of non-compliant AI systems**.

06

The lack of a unified ecosystem of enforcement for new digital-related EU legislation may lead to significant divergences. A unified enforcement agency, strengthening the proposed EU AI Board and drawing on existing resources and processes at national level, appears absolutely necessary. In line with EU consumer protection law and the GDPR, a meaningful enforcement process should also include individual and collective redress mechanisms.

3.7 ALIGN DATA TRANSFER RULES WITH THE STATED GOALS OF THE AI ACT

Data flows are fundamental for the development and deployment of AI technologies. Upcoming EU legislation in relation to data transfers, such as the proposed Data Act, **appears relatively inconsistent with the goal of increasing the uptake of AI systems in the EU**, due to its potential implications for the free flow of data between EU and non-EU countries.

Indeed, a recent CEPS policy brief indicates a recent 'shift in the EU's approach to the wider data economy, from championing the free flow of non-personal data in the context of the 2016 DSM strategy to the introduction of specific requirements for governing and limiting data transfers in the context of the Data Act' (Perarnaud and Fanni, 2022).

This approach materialises in the Data Act via a new obligation for cloud providers to prevent international transfers of non-personal data where such transfers could create conflicts with EU and Member States' laws. New legal restrictions to cross-border data flows may be justified, but would require significant international cooperation, especially as more and more countries adopt data localisation requirements (including India).

The DGA also introduces new GDPR-like rules for international transfers of non-personal data, which could apply to cloud providers. It provides for a self-enforcement approach, however, meaning that cloud service providers will be 'left with the responsibility to decide, in the absence of a relevant international agreement, whether foreign governments requesting access to or transfer of the clients' data provide sufficient rule of law guarantees' (Baloup, 2022).

In parallel, the EDPB has recently released new guidelines on the interplay between the (extra-)territorial scope of the GDPR and its provisions on international transfers. These guidelines clarify what type of processing activities can qualify as personal data transfers, stating in particular that processing will be considered a transfer, regardless of whether the importer established in a third country is already subject to the GDPR's territorial

scope (Article 3). The guidelines therefore create additional complexity as 'organizations located anywhere on the globe and subject to the jurisdiction of the GDPR must adopt a transfer mechanism when sending personal data to a separate organization outside of EU territory' (Fennessy, 2021).

These recent developments point to a **clear lack of consistency in relation to the EU's approach towards the governance of international data flows** and its political ambition to strengthen the development of AI technologies in Europe.

07

New rules and guidelines governing international transfers of non-personal data could impact data flows and the uptake of AI systems in the EU. New requirements for data flows, notably for cloud providers in the context of the proposed Data Act, should acknowledge and better assess their impact on EU and cross-border AI development.

3.8 SAFEGUARD EXEMPTIONS FOR SCIENTIFIC RESEARCH

The AI Act does not offer a comparable exemption for scientific projects to Article 89 GDPR, which provides for exceptions to data protection rules for research purposes. This could mean that AI scientists run the risks of being subject to the same obligations as AI providers when publishing their AI models in academic settings. The AI Act could clarify that publishing models and putting them online for free (i.e. open source) would not count as putting them on the market.

As stated by several MEPs, including in the opinion of the ITRE Committee, there is a need to ensure that the AI Act does not undermine research and development (R&D) around AI systems. This regulation should apply only when scientific projects are expected to lead to or entail placing an AI system on the market. **AI systems developed for the sole purpose of scientific research should not be constrained by the same regulatory framework** but should respect recognised ethical standards.

The Council has discussed similar exemptions for scientific research, stating for instance under the Slovenian presidency that 'it is therefore necessary to exclude from its scope AI systems specifically developed and put into service for the sole purpose of scientific R&D and to ensure that the regulation does not otherwise affect scientific R&D activity on AI systems'. One of the challenges then becomes to define which AI systems fall within the scope of this 'sole purpose' criterion. A recent paper by Kazim et al. (2021) indeed

highlights **the need to make sure that the exemption cannot be gamed in the form of structuring work as R&D**, when in fact it is work developed for a particular purpose.

08

There is a need to ensure that the AI Act does not undermine R&D around AI systems. This regulation should apply only when scientific projects are expected to lead to or entail placing an AI system on the market. AI systems developed for the sole purpose of scientific research should not be constrained by the same regulatory framework. Yet, the exemption needs to be drafted so as to prevent it being used a means to circumvent AI Act requirements by structuring work as R&D.

4. REFERENCES

Baloup, J. (2022), 'The Data Act or the final piece to create a comprehensive legal framework for international transfers of data', European Law Blog, 14 June, https://europeanlawblog.eu/2022/06/14/the-data-act-or-the-final-piece-to-create-a-comprehensive-legal-framework-for-international-transfers-of-data/.

Bertuzzi, L. (2022), 'The data provisions in the EU's upcoming Big Tech law', IAPP, 22 March, https://iapp.org/news/a/the-data-provisions-in-the-eus-upcoming-big-tech-law/

BEUC (2021), *Regulating AI to protect the consumer*, Position Paper on the AI Act, Brussels, 7 October, https://www.beuc.eu/publications/beuc-x-2021-088_regulating_ai_to_protect_the_consumer.pdf.

Casarosa, F. (2022), 'Cybersecurity certification of Artificial Intelligence: a missed opportunity to coordinate between the Artificial Intelligence Act and the Cybersecurity Act', *International Cybersecurity Law Review*, Vol. 3, No 1, pp. 115–130, https://doi.org/10.1365/s43439-021-00043-6.

Codagnone, C. (2022), *Identification and assessment of existing and draft EU legislation in the digital field*, Report commissioned by the AIDA Special Committee, European Parliament, https://www.europarl.europa.eu/RegData/etudes/STUD/2022/703345/IPOL_STU(2022)703345_EN.pdf.

Ebers, M. (2021), 'Standardizing AI—The case of the European Commission's proposal for an artificial intelligence act', *Cambridge handbook of artificial intelligence: global perspectives on law and ethics*, https://ssrn.com/abstract=3900378.

Edwards, L. (2022), *Regulating AI in Europe: four problems and four solutions*, Ada Lovelace Institute, 31 March, https://www.adalovelaceinstitute.org/report/regulating-ai-in-europe/.

Engler, A. (2021), 'Platform data access if a lynchpin of the EU's Digital Services Act', Brookings, 15 January, https://www.brookings.edu/blog/techtank/2021/01/15/platform-data-access-is-a-lynchpin-of-the-eus-digital-services-act/.

Fennessy, C. (2021), 'New EDPB guidelines define international transfers: Dancing in place', IAPP, 29 November, https://iapp.org/news/a/new-edpb-guidelines-define-international-transfers-dancing-in-place/.

Georgieva, T., Timan, T. and Hoekstra, M. (2022), *Regulatory divergences in the draft AI act: Differences in public and private sector obligations*, Study, European Parliamentary Research Service (EPRS), Brussels, https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729507/EPRS_STU(2022)729507_EN.pdf.

Graef, I. and Husovec, M. (2022), *Seven Things to Improve in the Data Act*, SSRN, 7 March, http://dx.doi.org/10.2139/ssrn.4051793.

Greenleaf, G. (2021), 'The "Brussels effect" of the EU's "AI Act" on data privacy outside Europe', *Privacy laws & business,* No 171, pp. 3–7.

Husovec, M. and Derclaye, E. (2022), *Why the Sui Generis Database Clause in the Data Act Is Counter-Productive and How to Improve It?*, SSRN, 8 March, http://dx.doi.org/10.2139/ssrn.4052390.

Kazim, E., Güçlütürk, O., Almeida, D. et al. (2022), 'Proposed EU AI Act—Presidency compromise text: select overview and comment on the changes to the proposed regulation', *AI Ethics*, 27 June, https://doi.org/10.1007/s43681-022-00179-z.

Kerry, C., Meltzer, J., Renda, A., Engler, A. and Fanni, R. (2021), *Strengthening international cooperation on AI*, Progress report by the FCAI, Brookings and CEPS, 25 October, https://www.brookings.edu/research/strengthening-international-cooperation-on-ai/.

Leufer, D. (2021), 'Here's how to fix the EU's Artificial Intelligence Act', Access Now, 7 September, https://www.accessnow.org/how-to-fix-eu-artificial-intelligence-act/.

Muller, C., Dignum, V., Avramidou, M. and Fernández Peñalver, M. (2022), *AIA in-depth #1: Objective, Scope, Definition*, ALLAI report, 13 February, https://allai.nl/wp-content/uploads/2022/03/AIA-in-depth-Objective-Scope-and-Definition.pdf.

Muller, C., Talvitie, C. and van Ree, R. (2022), *AIA in-depth #2: Prohibited AI Practices*, ALLAI report, 24 February, https://allai.nl/wp-content/uploads/2022/03/AIA-in-depth-2-Prohibited-AI-Practices.pdf.

Muller, C., Schöppl, N., Avramidou, M., Talvitie, C. and Férnandez Peñalver, M. (2022), *AIA in-depth #3a: High-Risk AI Classification*, ALLAI report, 20 April, https://allai.nl/wp-content/uploads/2022/04/AIA-in-depth-3a-High-Risk-AI-Classification.pdf.

Perarnaud, C. and Fanni, R. (2022), *The EU Data Act: Towards a new European data revolution?*, CEPS Policy Insights, No 2022-05, https://www.ceps.eu/ceps-publications/the-eu-data-act/.

Prufer, J. and Graef, I. (2021), *Governance of Data Sharing: a Law & Economics Proposal*, TILEC Discussion Paper No 2021-001, CentER Discussion Paper No 2021-004, http://dx.doi.org/10.2139/ssrn.3774912.

Renda, A. et al. (2021), *Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe*, European Commission, DG

CONNECT, 21 April, https://op.europa.eu/en/publication-detail/-/publication/55538b70-a638-11eb-9585-01aa75ed71a1.

Sartor, G. and Lagioia, F. (2020), *The impact of the General Data Protection Regulation on artificial intelligence*, European Parliamentary Research Service (EPRS) study, Brussels, June, https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf.

Storms, S., Valcke, P. and Kindt, K. (2019), 'Rage against the machine: does machine-to-machine communication fall within the scope of the confidentiality principle?', *International Journal of Law and Information Technology*, Vol. 27, No 4, pp. 372–408, https://doi.org/10.1093/ijlit/eaz012.

Taddeo, M., McCutcheon, T. and Floridi, L. (2019), 'Trusting artificial intelligence in cybersecurity is a double-edged sword', *Nature Machine Intelligence*, Vol. 1, No 12, pp. 557–560.

Varošanec, I. (2022), 'On the path to the future: mapping the notion of transparency in the EU regulatory framework for AI', *International Review of Law, Computers & Technology*, Vol. 36, No 2, pp. 95–117, https://doi.org/10.1080/13600869.2022.2060471.

Veale, M. and Zuiderveen Borgesius, F. (2021), 'Demystifying the Draft EU Artificial Intelligence Act — Analysing the good, the bad, and the unclear elements of the proposed approach', *Computer Law Review International*, Vol. 22, No 4, pp. 97–112. https://doi.org/10.9785/cri-2021-220402.

CEPS
PLACE DU CONGRES 1
B-1000 BRUSSELS