STUDY

Requested by the AIDA special committee

European Parliament

Identification and assessment of existing and draft EU legislation in the digital field

Relevant to the mandate of the AIDA Special Committee

Policy Department for Economic, Scientific and Quality of Life Policies
Directorate-General for Internal Policies
Authors: C. CODAGNONE, G. LIVA, T. RODRIGUEZ DE LAS HERAS BALLELL
PE 703.345 - January 2022

EN

Identification and assessment of existing and draft EU legislation in the digital field

Relevant to the mandate of the AIDA Special Committee

Abstract

This study aims to deliver to the AIDA committee an overview of all existing and planned EU legislation in the digital field, together with an assessment of the interactions amongst these pieces of legislation.

The analysis of the interplay between the legal acts, which regulate the development, placing on the market, and use of AI systems, or other AI-related aspects, has revealed intended or inadvertent regulatory gaps that should be addressed.

This document was provided by the Policy Department for Economic, Scientific and Quality of Life Policies at the request of the special committee on Artificial Intelligence in a Digital Age (AIDA).

This document was requested by the European Parliament's special committee on Artificial Intelligence in a Digital Age (AIDA).

AUTHORS
Cristiano CODAGNONE, Open-Evidence
Giovanni LIVA, Open-Evidence
Teresa RODRIGUEZ DE LAS HERAS BALLELL, Universidad Carlos III de Madrid

ADMINISTRATOR RESPONSIBLE
Matteo CIUCCI

EDITORIAL ASSISTANT
Irene VERNACOTOLA

LINGUISTIC VERSIONS
Original: EN

ABOUT THE EDITOR
Policy departments provide in-house and external expertise to support European Parliament committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny over EU internal policies.

To contact the Policy Department or to subscribe for email alert updates, please write to:
Policy Department for Economic, Scientific and Quality of Life Policies
European Parliament
L-2929 - Luxembourg
Email: Poldep-Economy-Science@ep.europa.eu

Manuscript completed: January 2022
Date of publication: January 2022

This document is available on the internet at:
http://www.europarl.europa.eu/supporting-analyses

DISCLAIMER AND COPYRIGHT

For citation purposes, the publication should be referenced as: Codagnone, C. et Al., 2022, *Identification and assessment of existing and draft EU legislation in the digital field*, Study for the special committee on Artificial Intelligence in a Digital Age (AIDA) , Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg.

CONTENTS

LIST OF ABBREVIATIONS

AGRI	Agriculture and Rural Development committee
AI	Artificial Intelligence
AIDA	Artificial Intelligence Data Analysis
BOE	Boletín Oficial del Estado
B2B	Business to Business
B2C	Business to Consumer
B2G	Business to Government
CSIRTs	Computer-Security Incident Response Teams
DA	Data Act
DGA	Data Governance Act
DLT	Distributed Ledger Technology
DMA	Digital Market Act
DSA	Digital Service Act
DSM	Digital Single Market
EAA	European Economic Area
EBA	European Banking Authority
EC	European Commission
ECOSOC	Economic and Social committee
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
eID	Electronic Identity
eIDAS	Electronic Identification Authentication and Signature

ENISA	European Union Agency for Cybersecurity
EP	European Parliament
EU	European Union
EU VOEC	European Union Value added tax On E-Commerce
EuroHPC	European High Performance Computing
FAIR	Findable, accessible, interoperable and reusable
FAO	Food and Agriculture Organisation of the United Nations
FISMA	Federal Information Security Management Act
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
G2B	Government to Business
ICT	Information and Communication Technologies
IoT	Internet of Things
ITRE	EP Committee on Industry, Research, and Energy
MFF	Multiannual Financial Framework
MOSS	Mini One Stop Shop
M2M	Machine-to-Machine
NIS	Network and Information Systems
PSI	Public Sector Information
P2B	Platform to Business
SME	Small and Medium-sized Enterprises
SWD	Staff Working Document
TEU	Treaty on European Union
TRADE	Directorate General for Trade

TTC	Trade and Technology Council
UN	United Nations
US	United States
VAT	Value Added Tax
5G	Fifth (5) Generation
6G	Sixth (6) Generation

LIST OF TABLES

LIST OF FIGURES

LIST OF BOXES

EXECUTIVE SUMMARY

Background

Between the first communication on Artificial Intelligence (European Commission, 2018) and the launch of the Policy Programme 'Path to the Digital Decade' (September 2021), the European Commission has been very active in the domain of digital transformation[1]. This fast-changing legislative production is matched by an even faster pace of development in digital technologies and their applications. In its draft report, the AIDA special Committee stressed the need for new digital regulations to harmonise the European digital single market, closing some of the regulatory gaps which cumulated toward global competitors and preserving its digital sovereignty. Due to rapid technological development, the text calls for an adaptable, principle-based, and future-proof legislation.

The proposal of the AI Act represents the first initiative providing a legal framework for Artificial Intelligence. Together with the other proposed legislations (Digital Service Act, Digital Market Act, Data Governance Act, and Data Act) and the GDPR, the new AI Act will shape the EU digital policy. At the same time, it is considered to influence other legislators in third countries. However, this ongoing legislation in the digital field is becoming increasingly complex, making at times regulatory coherence and consistency hard to be achieved. There are several interplays between the AI Act and the other existing or upcoming legislations that have not received enough attention.

Aim

This situation justifies AIDA Committee request for an overview and a taxonomy of digital legislation and of possible regulatory gaps. Against this background, the overall objective of this study is to obtain 'an overview of all existing and planned EU legislation in the digital field, together with an assessment of the interactions amongst these pieces of (draft) legislation'. To achieve this objective this study produced three main outputs. First, a systematic overview of existing and upcoming digital regulations and directives by vertical policy domains was produced. Second, the interplay between the main and more important legislative acts and their coherence was analysed and systematised. Third, regulatory gaps were identified and placed into a taxonomy comprising three categories: a) identified in a Commission's document and already addressed under an upcoming or programmed legislative work; b) identified in a Commission's document, but not yet addressed under an already and upcoming or programmed legislative work; c) never addressed so far.

Key Findings

The analysis of the interplay between the selected legal acts, directly or indirectly regulating the development, placing on the market, putting into service or use of AI systems, or other AI-related aspects, or issues arising from algorithmic processes and decision-making may reveal intended or inadvertent regulatory gaps.

Gaps have been first identified within the AI Act. By delimiting the scope of application, the AI Act delineates the contours of the regulatory perimeter, excluding or not addressing certain purposes, uses or sectors. In that regard, the AI Act may leave certain gaps uncovered, such as, for instance, the social

[1] As can be seen in the long preamble of the Draft Final Report on Artificial Intelligence (2020/2266(INI)) released of 2 November 2021 by the Special Committee on Artificial Intelligence in a Digital Age (see AIDA, 2021a, pp. 3-8).

scoring leading to detrimental treatment, the biometric identification systems, and military purpose AI systems. Moreover, as the AI Act is based on a purpose-specific approach, such a scoping strategy raises the question of general-purpose and multi-purpose AI systems.

The interplay between the AI Act as the core component of the AI regulatory framework and other legal acts have revealed some doubtful areas. First, the compliance or non-compliance of certain obligations laid down by the AI Act may trigger (rebuttable) presumptions for the purposes of attributing liability and allocating the burden of proof. Additionally, it is not clear to which extent the designation as a high-risk is consistent throughout all relevant regulations and whether the high-risk category should lead to the application of strict liability regimes in any event. Overall, the adequacy of the liability rules to properly address and compensate damages and losses caused by AI system is a critical issue in the shaping of a flawless regulatory framework for AI in the EU.

The interplay between the liability exemption – under e-Commerce Directive as revisited in the DSA – and the intensive use of algorithmic decision-making in content moderation, notice and removal, complaint-handling or conflict solving is another critical issue identified. There are friction points in several aspects. For instance, it is not clear whether the deployment of a large-scale algorithm content moderation system may entail *de facto* general monitoring. Whether the poor performance of algorithmic voluntary measures failing to detect (illegal/inappropriate) content should be interpreted as explicit operators' knowledge and trigger the duty to react and the resultant liability. In addition, it is unclear whether Article 5(3) DSA goes beyond the platform's liability of information of the trader and might entail that the platform operator is placed at the position of the trader as contracting party vis-à-vis the consumer.

In the context of contracts concluded by electronic means, while the e-Commerce Directive recognises the validity and enforceability of such contracts, it remains unclear whether self-executed contracts (smart contracts meeting the requirements to be qualified as legal contracts) shall not be denied legal effects solely on the grounds that are coded in machine language and self-executable. This might fill a gap that has not yet been addressed in the EU. Divergent national legislation on this issue would fragment the internal market in the development of AI/algorithms applications.

A thorough analysis of the regulatory gaps in relation to algorithmic transparency should jointly consider Article 22 GDPR, the transparency requirements laid down in the AI Act, the provision on ranking of the P2B Regulation or the provisions on recommender systems for very large platforms in the DSA. The joint analysis of these legal acts that we carried out confirms that the transparency, disclosure, and explanation of parameters, criteria, or conditions under which certain algorithm-driven systems work is a fundamental horizontal policy decision that should be taken at the EU level and where existing and proposed acts show little coherence. Comparing the scope of application of the relevant provisions as set out in the above-referred legal acts (GDPR, DSA, P2B Regulation) does show an incomplete picture with some regulatory gaps needing attention.

The interplay between the AI Act and the GDPR is multi-fold and conspicuous. The AI Act acknowledges that its provisions are without prejudice of any other EU legal acts the operators of AI systems must abide by data protection regime (Recital 41 AI Act). And more explicitly, the AI Act (Recital 41) stresses that it should not be interpreted as providing the legal ground for processing of personal data. But such a generic statement of compatibility between the AI Act and the personal data protection regime may not be sufficient to cover all possible use of data by AI systems. Therefore, more clarity in the AI Act as regards the processing of personal data is needed and, consequently, some regulatory gaps can be singled out.

There are also several interplays between AI and cybersecurity. First, machine-learning and deep-learning techniques, might aggravate the cybersecurity risks insofar as they render cyber-attacks better targeted, more destructive, and effective, and more elusive to prevention measures as they change and adapt to new counterattacking responses. Second, however, AI systems will enhance the effectiveness of preventive measures against cyber-attacks, serving as a shield against sophisticated cybersecurity breaches. Third, AI systems are exposed to vulnerabilities. Measures to ensure resilience, technical robustness, and cybersecurity in AI systems, and the ICT infrastructure, especially in critical and strategical sectors, are to be adopted and effectively implemented. These interactions between AI and cybersecurity lead to varied interplays between the AI Act and the Cybersecurity Act, and the AI Act and the NIS2 Directive that may reveal certain overlaps or regulatory gaps.

Finally, the present study has identified other gaps of potential implementation issues in the Open Data Directive in relation to the proposed Data Governance Act, in the Database Directive, in the P2B Regulation, in the DSA and in the DMA. In conclusion, in this study the authors claim that regulation of the digital domain in Europe should strike a balance between protecting fundamental rights, promoting innovation, being ambitious but at the same time coherent without adding unnecessary layers of complexity. It seems, however, that in the building of digital constitutionalism, coherence and simplicity have been at least partially overlooked.

INTRODUCTION

Rationale and objectives

In the four years elapsed between the first communication on Artificial Intelligence (European Commission, 2018) and the launch of the Policy Programme 'Path to the Digital Decade' on September 2021, the Commission has been very active in the domain of digital transformation with both communications and legislative acts[2]. In the past two years, several proposals for new regulations have been presented. At the time of publication (December 2021), some important proposals are still being discussed and modified.

This fast-changing legislative production is matched by an even faster pace of development in digital technologies and their applications. In its draft report, AIDA special Committee stressed the need for new digital regulations to harmonise the European digital single market, closing some of the regulatory gaps which cumulated toward global competitors and preserving its digital sovereignty. Due to rapid technological development, the text calls for legislation that: '[…] should always be swiftly adaptable, principle-based and future-proof, while adopting a risk-based approach; stresses, furthermore, the importance of legal certainty and, consequently, the need for robust, practical and unambiguous applicability criteria, definitions and obligations in all legal texts '(AIDA, 2021a, p. 24).

This situation justifies AIDA Committee request for an overview and a taxonomy of digital legislation and of possible regulatory gaps. Against this background, the overall objective of this study is to obtain 'an overview of all existing and planned EU legislation in the digital field, together with an assessment of the interactions amongst these pieces of (draft) legislation'. To achieve this objective this study produced three main outputs. First, a systematic overview of existing and upcoming digital regulations and directives by vertical policy domains was produced. Second, the interplay between the main and more important legislative acts and their coherence was analysed and systematised. Third, regulatory gaps were identified and placed into a taxonomy comprising three categories: a) identified in a Commission's document and already addressed under an upcoming or programmed legislative work; b) identified in a Commission's document, but not yet addressed under an already an upcoming or programmed legislative work; c) never addressed so far.

To this purpose, a team comprised by two policy analysts (Open Evidence) and one legal expert (Professor Teresa Rodriguez de las Heras Ballell)[3] were supervised by the lead author Cristiano Codagnone (Open Evidence). The brief description of the team is instrumental to transparently make the following distinction about the contents of this study. Most of this introduction, chapters 1, 2, 3, 4, and 5 are strictly based on legal analysis and are, as much as possible, factual. The next section of this introduction, as well as parts of the conclusions in chapter 6, contain considerations by the lead author that are based on extra-legal literature (i.e., political, and socio-economic) and to some extent should be read as subjective appraisal and interpretation. Some of such considerations are also placed in boxes to flag their different nature to the reader in chapters containing strictly legal analysis.

[2] As can be seen in the long preamble of the Draft Final Report on Artificial Intelligence (2020/2266(INI)) released of 2 November 2021 by the Special Committee on Artificial Intelligence in a Digital Age (see AIDA, 2021a, pp. 3-8).

[3] Professor of Commercial Law at Universidad Carlos III de Madrid.

Some general considerations

As noted, 'the world stands on the verge of the fourth industrial revolution' (AIDA, 2021a, p. 8), where data are the new oil and algorithms the new machines. Within this fourth industrial revolution AI is the pivotal and cornerstone technology, for it will become the steering centres of surrounding data layers, and by 2030 is expected to contribute more than EUR 11 billion to the global economy (AIDA, 2021x, p. 9).

Indeed, the proposal of the AI Act, as a complement to GDPR, has been defined by the European Data Protection Supervisor as 'the first initiative, worldwide, that provides a legal framework for Artificial Intelligence'. This act is considered 'one of the most influential regulatory steps taken so far internationally' (Floridi, 2021, p. 216). Together with the GDPR, and with the other proposed regulations (Digital Service Act, Digital Market Act, Data Governance Act, and Data Act) it will make up a hexagon envisaging the coming of a new EU Digital Constitutionalism (Celeste, 2019; De Gregorio, 2021) for better and more sustainable lives, work, and businesses. All these acts tend to be 'extra-territorial', or technically to have territorial extension (Scott, 2014) with the consequence that market players must deal with EU regulations regardless of where they operate if such operations affect EU citizens. This is considered the source of the so-called Brussels effect (Bradford, 2020). It is an approach where legal act are no longer applicable only on the basis of the territory when an activity takes place (Floridi, 2014).

It must be anticipated, however, that this ongoing legal construction in digital constitutionalism is becoming increasingly complex, making at times regulatory coherence and consistency, two dimensions where EU law doesn't always score well (Brownsword, 2019, p. 155), hard to be achieved. Many impact assessments carried out by the Commission before unveiling the AI Act could not analyse its many interplays with other existing or upcoming legislative acts. In the AI Act Impact Assessment, only a few paragraphs are devoted to the analysis of its coherence with other legislative acts (European Commission, 2021, pp. 84-85). In this respect it is worth mentioning that recently the Regulatory Scrutiny Board rejected the impact assessment supporting the proposal for the Data Act[4]. This confirms the complexity of the digital dossier and in view of such complexity, in this report, leaving aside visions of digital constitutionalism and the related Brussels effect, interplays and coherence are considered quite thoroughly.

Scope and contents

The scope of the report follows a funnel approach starting with a wide overview of relevant legislative and other initiatives, then narrowing down the analysis of interplays to main selected areas and finally reducing its scope when considering regulatory gaps.

The initial wide overview, presented in chapter 1, covers the following vertical policy domains:

1) ICT services, infrastructures, and networks;

2) Trust and security;

3) Consumer protection and competition;

4) Online services and e-commerce;

5) Data protection and governance;

[4] See Bertuzzi, L. 'Draft impact assessment sheds some light on upcoming Data Act', Euractiv, 21 November 2021. See: (https://www.euractiv.com/section/data-protection/news/leak-draft-impact-assessment-sheds-some-light-on-upcoming-data-act/).

6) Copyrights and audio-visuals; and

7) e-Government.

The initiatives[5] under each of this vertical policy domains present some overlaps especially between: a) Trust and Security with Data Governance and Management; b) Consumer Protection and competition with Online Services and e-Commerce; c) between almost all seven domains and AI. Accordingly, the analysis of interplays is performed for three more broadly defined policy areas: data protection and governance (Chapter 2); digital services and markets (chapter 3); and AI (Chapter 4).

In the following, the analysis of regulatory gaps in chapter 5 focuses on AI as such (Section 5.1), on the interplay of AI with GDPR and the proposed ePrivacy Regulation (Section 5.2), and on the interplay between AI and Cybersecurity (Section 5.3). Other relevant gaps are residually reviewed in Section 5.4, whereas the synoptic taxonomy of regulatory gaps is presented in Section 5.5. Chapter 6 concludes with some general considerations and recommendations.

[5] In Chapter 1 of the study, we use the extended and official names of the legislations (e.g., General Data Protection Regulation (EU) 2016/679) together with the hyperlinks. In the following chapters we used abbreviations that are commonly used (e.g., GDPR).

1. OVERVIEW OF EXISTING AND UPCOMING REGULATION

1.1. Dimensions used for the overview and their rationale

The EU procedures and acts in the digital domain reviewed in this study are categorised along three dimensions: their type, status, and vertical policy domain. First, there are two broad types: legislative and non-legislative, including intergovernmental alliances and conclusions of international summits. Although the latter does not have a legislative nature, it nonetheless may lead to future legislative initiatives or be impacted by them or by judicial decisions based on existing and future legislation. For instance, the EU-US Trade and Technology Council (TTC) may solve the earlier problems emerged regarding the EU-US Privacy Shield or be affected by the provisions of upcoming acts such as the Digital Governance Act and its implications on international data transfer (see Text Box 1, p. 36). A second distinction is between already existing legal acts, draft legislative acts with official proposals having been presented, and announced legislative acts. Third, we use seven vertical policy domains (ICT services, infrastructures, and networks; Trust and security; Consumer protection and competition; Online services and e-commerce; Data protection and governance; Copyrights and audio-visuals; e-Government).

Any new conceptualisation faces a trade-off between having enough descriptive power and empirical basis and avoiding the introduction of categories not easily recognised by practitioners. As such, it requires hard choices of inclusion and exclusion of items (Bailey, 1994)[6]. We have tried to strike a compromise with respect to this trade-off, although some potential overlaps and possible alternative choices remain that we transparently acknowledge here. First, one could further split initiatives by separating online services and their management from consumer protection and competition. We refrained from doing so because the analysis of interplays in chapter 3 will show that they are related. Second, we could have included one more vertical domain for initiatives related to VAT and other issues concerning tax and payments. Doing so, however, would have left a category with only two items, which from an empirical point of view suggests that they should be rather grouped with another category. Third, instead of having a single 'data protection and governance' category, we could have split it in two sub-categories, such as 'data protection and governance' and 'data management'. This aspect, however, will be specifically addressed in the next chapters focussed on the interplay and coherence of the main pieces of digital legislation.

Let us now map our review against all initiatives announced in the European Digital Strategy (2020a) in the Table 1 below. The parts in blue indicate our additions as compared to the content of the strategy.

[6] A sound typology or taxonomy is one that (i) have descriptive power and be empirically grounded, (ii) reduce complexity, and (iii) identify similarities and differences. Robust typologies and taxonomies should be based on intentional definitions that establish the necessary and sufficient conditions for a 'thing' being a member of a specific set. The disadvantage of such definitions is that empirical reality is always more complex and nuanced than any of such definitions could capture; using the intentional approach may entail excluding items from a specific set of 'things' in ways that may appear artificial or arbitrary to practitioners. The alternative are so called 'ostensive definitions' that simply pragmatically list what is included in them. Their advantage is that they are more inclusive and reduce hard clear-cut choices and exclusions. Their disadvantage is that, if they are too loose and encompassing, they become trivial with limited descriptive power and do not reduce complexity as they group together entities that are similar with regard to very few characteristics.

Table 1: Mapping our review against the Digital Strategy

Technology that works for people	
Legislative	Non legislative
AI Act and ePrivacy	White Paper on AI
Revised regulation on supercomputing	Building and deploying cutting-edge joint digital capacities in AI, cyber, super and quantum computing
Revision of broadband cost reduction directive	Updated Action Plan on 5G and 6G, a new Radio Spectrum Policy Programme. 5G corridors for connected and automated mobility
Review of the Security of Network and Information Systems (NIS) Directive	European Cybersecurity strategy
	Digital Education Action Plan and Skills Agenda
	A reinforced EU governments interoperability strategy
Fair and competitive economy	
Legislative	Non legislative
Legislative framework for data governance	European data strategy
Digital Service Package	Evaluation of fitness of EU competition rules
EU VAT for e-commerce package	Communication on Business Taxation for the 21st century
Payment services Directive	Framework for competitive & secure Digital Finance
	Industrial strategy package
	Delivering a new Consumer Agenda
Open, democratic, sustainable society	
Legislative	Non legislative
Revision of eID regulation	
Digital Service Package as instrument to deepen internal market for digital services	
European health data space	Promotion of electronic health records
	Media and audiovisual action plan
	European Democracy action plan
	Destination Earth (a 'Digital Twin of the Earth')
	A circular electronics initiative
	Initiatives to achieve climate-neutral, highly energy efficient and sustainable data centres
The International Dimension	
Legislative	Non legislative
	Global Digital Cooperation Strategy
	White Paper on foreign subsidies
	Digital for Development Hub
	A strategy for standardisation
	Action plan to promote the European bilateral and multilateral relations

Source: Own elaboration on European Commission (2020a).

As will be appreciated in Table 2 in next section, we have covered all the legislative initiatives mentioned in the strategy and left out all the other 23 non legislative initiatives, the majority of which we have discussed elsewhere (Codagnone et al., 2021).

1.2. Synoptic table by policy areas

In the table below the seven policy domains are the heading of the columns, whereas the colouring of the cells is self-explanatory (blue: existing legislation, light blue: presented legislative proposals; green: announced legislative acts; orange: alliances and treaties).

Table 2: Overview of the EU digital acts and proposals by policy domains

ICT services, infrastructure, networks	Trust and security	Consumer protection and competition	Online services and e-commerce	Data protection and governance	Copyrights and audiovisuals	e-Government
Regulation on High Performance Joint Undertaking (EU) 2021/1173[1]	EU Cybersecurity Act Regulation (EU) 2019/881[2]	Regulation on platform-to-business relations (P2B Regulation) (EU) 2019/1150[3]	EU VAT for e-commerce package (EU VOEC) [4]	Open Data Directive (EU) 2019/1024[5]	Directive on Copyrights and related rights in the DSM Directive EU (2019) 790[6]	E-invoicing Directive (EU) 2014/55[7]
European electronic communications Code Directive (EU) 2018/1972[8]	Network and Information Security (NIS) Directive EU 2016/1148[9] *[under revision]*	Roaming Regulation (EU) 2017/920[10] *[under revision*	Payment Services Directive (EU) 2015/2366[11]	General Data Protection Regulation (GDPR) (EU) 2016/679[12]	Satellite and Cable II Directive (EU) 2019/789[13]	Electronic identification rules - eIDAS Regulation (EU) No 910/2014[14] *[under revision]*
Broadband Cost Reduction Directive (EU) 2014/61[115] *[under revision]*	ePrivacy Directive 2002/58/EC	Measures concerning open internet access Regulation (EU) 2015/2120[17]	e-Commerce Directive 2000/31/EC[18]	Regulation on the free flow of non-personal data (EU) 2018/1807[19]	Portability Regulation (EU) 2017/1128[20]	Digitalisation of visa procedures[21]
Regulation establishing the European Cybersecurity Competence Centre and Network 2021/887[22]	Legislative proposal for an Artificial Intelligence Act COM 2021/206[16]	Proposal for a Digital Markets Act COM/2020/842[24]	Geo-Blocking Regulation (EU) 2018/302[25]	Directive on certain aspects concerning contracts for the supply of digital content and digital services 2019/770[26]	Radio Equipment Directive 2014/53/EU[27]	

Proposal on a pilot regime for market infrastructures based on distributed ledger technology[28]	Proposal for a Regulation on a high common level of cybersecurity Directive COM(2020) 823[23]	Proposal for a Regulation on Markets in Crypto-assets COM/2020/593[30]	Proposal for a Digital Services Act COM/2020/825[2] [31]	Data Governance Act (DGA) COM/2020/767[32]	Database Directive 96/9/EC[33] *[under revision]*
Legislative proposal on building an EU space-based global secure communication system[34]	Proposal for Regulation on Privacy and Electronic Communications[29] *[revision of ePrivacy Directive]*	Common charges for mobile phones and similar devices[36]	Legislative proposal on a Single Market Emergency Instrument[37]	European Data Act[38]	
European Chips Act[39]	Proposal on a Regulation on Machinery products COM/2021/202[35]	New design requirements and consumer rights for electronics[41]		European Health Data Space[42]	
Declaration of the Industrial Alliance for Processors and Semiconductor Technologies[44]	Proposal for a Regulation on digital operational resilience for the financial sector[40]	Multimodal digital mobility services[46]		European Alliance for Industrial Data, Edge and Cloud[43]	
EU-US Trade and Technology Council (TTC) [47]	European Cyber Resilience Act[45]				

Table 2 endnotes

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R1173.
[2] https://eur-lex.europa.eu/eli/reg/2019/881/oj.
[3] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019R1150.
[4] https://ec.europa.eu/taxation_customs/modernising-vat-cross-border-e-commerce_en.
[5] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L1024.
[6] https://eur-lex.europa.eu/eli/dir/2019/790/oj.
[7] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014L0055.
[8] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L1972.
[9] https://eur-lex.europa.eu/eli/dir/2016/1148/oj.
[10] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32017R0920.
[11] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L2366.
[12] https://eur-lex.europa.eu/eli/reg/2016/679/oj.
[13] https://eur-lex.europa.eu/eli/dir/2019/789.
[14] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG.
[15] https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32014L0061.
[16] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.
[17] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2015.310.01.0001.01.ENG.
[18] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32000L0031.
[19] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1807.
[20] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R1128.
[21] https://www.europarl.europa.eu/legislative-train/theme-promoting-our-european-way-of-life/file-digitalisation-of-visa-procedures#:~:text=Digitalisation%20of%20visa%20procedures%20%2F%20after%202021%2D09&text=The%20new%20Pact%20on%20Migration,to%20submit%20visa%20applications%20online.
[22] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0887.
[23] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:823:FIN.
[24] https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A842%3AFIN.
[25] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32018R0302.
[26] https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32019L0770.
[27] https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=celex:32014L0053.
[28] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0594.
[29] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010.
[30] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593.
[31] https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN.
[32] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767.
[33] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31996L0009.
[34] https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-building-an-eu-space-based-global-secure-communication-system.
[35] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0202.
[36] https://ec.europa.eu/commission/presscorner/detail/en/IP_21_4613.
[37] https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-single-market-emergency-instrument.
[38] https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-data-act.
[39] https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-european-chips-act-(semiconductors).
[40] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595.
[41] https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-design-requirements-and-consumer-rights-for-electronics.
[42] https://www.europarl.europa.eu/legislative-train/theme-promoting-our-european-way-of-life/file-european-health-data-space.
[43] https://ec.europa.eu/growth/industry/strategy/industrial-alliances/european-alliance-industrial-data-edge-and-cloud_it.
[44] https://ec.europa.eu/growth/industry/strategy/industrial-alliances/industrial-alliance-processors-and-semiconductor-technologies_it.
[45] https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-european-cyber-resilience-act.
[46] https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-multimodal-digital-mobility-services.
[47] https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_21_4951.

1.3. Short description of items

1.3.1. ICT services, infrastructure, networks

Regulation on High Performance Computing Joint Undertaking (EU) 2021/1173

Regulation (EU) 2021/1173 was formally adopted in July 2021. It repeals Regulation (EU) 2018/1488, which established the EuroHPC Joint Undertaking as a legal and financial framework, pooling resources from the European Union (EU), 32 countries and two non-governmental members[7]. The new legal act introduced modifications to adapt the Regulation to the programmes in the framework of the Multiannual Financial Framework (MMF) 2021-2027 while maintaining European Commission's priorities. This regulation strengthens research and innovation capabilities, the development of a supercomputing infrastructure ecosystem and the acquisition of world-class supercomputers by means of a joint undertaking. It aims at developing, deploying, extending, and maintaining in the EU a world-leading federated, secure, and hyper-connected supercomputing, quantum computing, service, and data infrastructure ecosystem.

European electronic communications Code Directive (EU) 2018/1972

Directive (EU) 2018/1972 was adopted by the European Union in December 2018 to set up a European Electronic Communications Code. This Directive establishes common EU rules and objectives on regulating the telecom industry and defines how providers of networks and/or services can be regulated by national authorities. The provisions include measures to stimulate investment in, and take-up of, very high-capacity networks in the European Union (EU), new spectrum rules for mobile connectivity and 5G, as well as changes to governance, the universal service regime, end-user protection rules, and numbering and emergency communication rules.

Broadband Cost Reduction Directive (EU) 2014/61 [under revision]

The Broadband Cost Reduction Directive (EU) 2014/61 entered into force in July 2016 to facilitate and incentivise the roll-out of high-speed electronic communications networks by lowering the costs of deployment with a set of harmonised measures. Furthermore, it facilitates shared use and deployment of physical infrastructure such as poles within several sectors, besides the electronic communication sector, such as energy and water. The report on the implementation of the Directive published in 2018 concluded that it was being transposed with significant delays in most Member States and its implementation has been inconsistent across the EU. The review of the Directive started in 2020 and it should provide investments adequate to achieve the new connectivity objectives.

Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (EU) 2021/887

Regulation (EU) 2021/887 entered into force in June 2021 with the aim of establishing the European competence centre for industrial competition, technology and research on cybersecurity and network of national coordination centres. The centre and network will strengthen Europe's role, leadership, and strategic autonomy in cybersecurity by maintaining and developing its capacities, including in the

[7] The European Technology Platform for High Performance Computing (ETP4HPC) and the Big Data Value (BDVA) associations.

digital single market. Furthermore, it will support critical infrastructure networks, software, and information systems used in the EU. Finally, it will enhance the EU's cybersecurity stance and convert cybersecurity into a competitive advantage.

Proposal for a Regulation on a pilot regime for market infrastructures based on distributed ledger technology COM/2020/594

Proposal COM/2020/594 was drafted by the Directorate General for Trade (TRADE) and by the Directorate General Financial Stability, financial services, and capital markets union (FISMA) of the European Commission. It aims to provide legal certainty, support innovation, consumer and investor protection and market integrity, and ensure financial stability, by establishing uniform requirements for operating DLT (Distributed Ledger Technology[8]) market infrastructures: permissions granted under this Regulation would allow market participants to operate a DLT market infrastructure and to provide their services across all Member States. This proposal was submitted to the Council of the European Union in September 2020 as well as for co-decision to the European Parliament.

European Chips Act

In September 2021, during the State of the Union letter of intent to the European Parliament President, Ursula von der Leyen and Maroš Šefčovič announced that the European Chip Act would be among the key new initiatives of the European Commission for 2022. The aim of the act is to better regulate the semiconductor market to innovate and increase the production of chips, the majority of which are imported from Asia and the United States. It would not only address the fostering of competition but also the creation of a European chip ecosystem, including manufacturing. The European Chips Act will try and integrate a coherent European vision and strategy and will provide a framework to avoid national subsidies, set conditions to protect European values and interests and define Europe's role in the global playing field.

Legislative proposal on building an EU space-based global secure communication system

In September 2021, during the State of the Union letter of intent to the European Parliament President, Ursula von der Leyen and Maroš Šefčovič announced that a legislative proposal on building an EU space-based global secure communication system would be among the key new initiatives of the European Commission for 2022. The system would ensure access to high-speed connectivity across the EU, relying on a multi-orbit space infrastructure including low earth orbit satellites. The system would also ensure highly secured connectivity and communication for governmental and commercial services, based on quantum encryption technologies; it would allow to better connect key infrastructure, to support crisis management, surveillance, and potential mass-market broadband applications. Furthermore, the system is intended to make sure that the EU would remain connected in case of cyber-attacks on the internet. The four objectives of the system would consist in: being independent from the non-EU initiatives, providing access to high-speed broadband to everyone across the EU, projecting Europe into the quantum security era, with protection against cyber- and hybrid threats; and keeping the continent connected including during attacks on the terrestrial infrastructure.

[8] A distributed ledger technology is a class of technologies which support the distributed recording of encrypted data.

Declaration of the Industrial Alliance for Processors and Semiconductor Technologies

The European Commission launched this alliance in July 2021. The overall objective of the Alliance is to identify current gaps in the production of microchips and the technology developments needed for companies and organisations to thrive. The desired impact will be to increase Europe's digital sovereignty, foster competitiveness, and address the growing demand of chips and processors. The two main lines are: The reinforcement of the European electronics design ecosystem and the establishment of the necessary manufacturing capacity.

EU-US Trade and Technology Council (TTC)

The European Union and the United States launched the EU-US Trade and Technology Council (TTC) at their summit in Brussels on 15 June 2021. The TTC serves as a forum for the EU and the US to coordinate approaches to key global trade, economic and technology issues, and to deepen transatlantic trade and economic relations based on shared democratic values. On 29 September 2021, an inaugural meeting of the TTC took place in Pittsburgh, USA. It was co-chaired by Commission Executive Vice-Presidents Margrethe Vestager and Valdis Dombrovskis, together with U.S. Secretary of State Antony Blinken, Secretary of Commerce Gina Raimondo, and Trade Representative Katherine Tai. Following the meeting, a joint statement was published, with a first set of concrete deliverables, i.e., declarations on investment screening, export controls, artificial intelligence, semiconductors, and global trade challenges. The next meeting of the TTC is planned in 2022.

1.3.2. Trust and security

EU Cybersecurity Act Regulation (EU) 2019/881

The Cybersecurity Act became effective in June 2019 and strengthens the EU Agency for cybersecurity (ENISA). It establishes an EU-wide cybersecurity certification framework for ICT products, services, and processes with the purpose of protecting the systems of organisations from cyberattacks. Companies doing business in the EU will benefit from having to certify their ICT products, processes, and services only once and see their certificates recognized across the European Union. Furthermore, this act fosters operational cooperation at an EU level by supporting Member States with cybersecurity incidents upon request and assisting in large-scale cross-border cyber-attacks.

Network and Information Security (NIS) Directive EU 2016/1148
[under revision]

The NIS Directive was adopted in 2016 with the goal to enhance cybersecurity across the European Union. It requires that EU Member States have certain national capabilities to supervise the cybersecurity of critical market operators in their country as well as for cross-border collaboration between EU countries. It sets up the designation of competent authorities, the computer-security incident response teams (CSIRTs), and the adoption of national cybersecurity levels. To provide greater support against threats from digitalization and cyber-attacks, the NIS Directive has been revised into the NIS 2 Directive. It would repeal the existing NIS Directive and broadens the scopes by introducing more security measures and enforcement. In April 2021, the Commission presented the NIS 2 Directive proposal to the Parliament lead committee on Industry, Research and Energy (ITRE).

ePrivacy Directive 2002/58/EC

The ePrivacy Directive was adopted in 2002 to safeguard the confidentiality of electronic communications in the EU. The ePrivacy Directive is a key instrument to protect privacy and it includes specific rules on data protection in the area of telecommunication in public electronic networks. It deals with the regulation of several important issues such as confidentiality of information, treatment of traffic data, spam and cookies. This Directive has been amended by Directive 2009/136, which introduces several changes, especially in what concerns cookies, that are now subject to prior consent.

Legislative proposal for an Artificial Intelligence Act COM 2021/206

Proposal COM 2021/206 was tabled by the European Commission in April 2021 as part of a legislative package on Artificial Intelligence (AI) overviewed by the Communication on Fostering a European approach to AI. The aim is to provide a legal framework for AI, proposes a single definition of AI, and provides legal certainty surrounding the scope of the act by enumerating computer sciences techniques and approaches that would be regulated. It identifies certain AI practices as harmful and prohibits them as well as lays a risk methodology for other types of AI. Furthermore, it proposes specific restrictions and safeguards in relation to certain uses of remote biometric identification systems.

Proposal for a Regulation on a high common level of cybersecurity Directive COM(2020) 823

Proposal COM(2020) 823, which was tabled by the European Commission in December 2020, aims to close the gaps on the limitations of the NIS Directive identified by the Impact Assessment. This proposal calls for increasing the level of cyber resilience across businesses operating in the EU, reduce discrepancies in resilience across the internal market, improve the level of situational awareness and the capability to prepare and respond to cybersecurity challenges in a coordinated way.

Proposal for a Regulation on Privacy and Electronic Communications COM(2017) 10 final *[revision of ePrivacy Directive]*

Proposal COM(2017) 10 was published by the European Commission on 10 January 2017. It repeals and replaces the ePrivacy Directive EU 2002/58 and aims to regulate privacy related topics while considering the rapidly evolving technological landscape, with issues such as confidentiality of machine-to-machine communication (Internet of Things) or the confidentiality of individuals' communication on publicly accessible networks. The existence of various challenges and gaps of the original Directive were raised including techniques to store and access information on users' equipment. Other parts of the Directive appear to have become technologically obsolete. Another key aspect under political discussion is related to storing and accessing data on a users' device, such as so-called Internet cookies. As of February 2021, the Council reached an agreement on its negotiating position, marking the beginning of negotiations with the European Parliament on the final text of the Regulation.

Proposal for a Regulation on Machinery products COM(2021) 202 final

Proposal COM(2021) 202 was tabled by the European Commission in April 2021 as part of a legislative package on Artificial Intelligence (AI) overviewed by the Communication on Fostering a European approach to AI. It aims to establish a regulatory framework for deploying machinery on the Single

Market of the EU. It fosters coordination of health safety requirements for machinery at a EU-level and proposes to increase users' trust in new, technological products.

Proposal for a Regulation on digital operational resilience for the financial sector COM/2020/595

Proposal COM/2020/595 was published in September 2020 as part of the European Commission's Digital Finance Strategy. This proposal builds on risk management requirements for ICT already developed by EU institutions and creates a cohesive approach across the EU, regulators, and financial entities. It aims to enhance the operational resilience of financial firms in case of severe ICT disruptions. Furthermore, it calls for the supervision of critical ICT third party providers, including cloud service providers, by European Supervisory Authorities.

European Cyber Resilience Act

In September 2021, during the State of the Union letter of intent to the European Parliament President, Ursula von der Leyen and Maroš Šefčovič announced that the European Cyber Resilience Act would be among the key new initiatives of the European Commission for 2022. It would be added to other proposals and directives about cybersecurity, specifically it aims to set common cybersecurity standards for connected devices.

1.3.3. Consumer protection and competition

Regulation on platform-to-business relations (P2B Regulation) (EU) 2019/1150

The so-called P2B Regulation was applied in July 2020 and aims to ensure fair and transparent rules for business users on online platforms. It set rules to ensure this and creates a predictable business environment for smaller businesses and traders on online platforms to avoid unfair contracts and trading practices in platform-to-business relations.

Roaming Regulation (EU) 2017/920
[under revision]

Regulation (EU) 2017/920 amended Regulation (EU) 2012/531 concerning rules for wholesale roaming markets and abolishing all roaming charges within the EEA. The Roaming Regulation is currently under revision with the proposed legislation COM/2021/85 final, presented in March 2021. The modified regulation would extend the current rules that will expire in 2022 for another 10 years and enhance the roaming services for travellers across the EU. The provisional agreement reached in December 2021[9] includes an adjustment of the maximum wholesale prices to ensure that the provision of retail roaming services at domestic prices is sustainable for operators throughout the EU. In addition, the revised regulation would include measures to ensure a good customer experience in terms of quality of service and access to emergency services, including for people with special needs.

[9] Available at: https://www.consilium.europa.eu/en/press/press-releases/2021/12/09/mobile-roaming-with-no-extra-fees-to-continue-as-presidency-reaches-deal-with-european-parliament/.

Measures concerning open internet access Regulation (EU) 2015/2120

Regulation (EU) 2015/2120 was published and adopted on 25 November 2015. This regulation amended Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the EU. The aim is to introduce safeguards for net neutrality, or the equal and non-discriminatory treatment of internet traffic and regulate mobile roaming services EU-wide by setting up a new pricing scheme. This pricing scheme abolishes surcharges without disrupting the market in the home or visited country. The regulation has applied since April 2016 and roaming charges were abolished from June 2017.

Proposal for a Digital Markets Act COM(2020) 842

Proposal COM(2020) 842 was tabled by the European Commission in December 2020. It aims to ensure open and contestable digital markets by preserving effective competition and ensuring that the large online platforms behave in a fair way. Furthermore, the proposal sets rules for platforms that act as 'gatekeepers', large platforms that have a durable position between business users and end users due to their impact on the digital markets. These platforms will have to comply with a series of obligations and prohibitions. This legislative proposal builds on the provisions of Regulation (EU) 2918/1150 (P2B Regulation).

Proposal for a Regulation on Markets in Crypto-assets COM(2020) 593

Proposal COM(2020) 593 was tabled by the European Commission in September 2020 and aims to amend Directive (EU) 2019/1937. It proposes to support innovation and fair competition by creating a framework for the issuance, and provision of services related to crypto assets. In addition, it aims to ensure a high level of consumer and investor protection and market integrity in the crypto-asset markets, as well as address financial stability and monetary policy risks that could arise from a wide use of crypto-assets and DLT-based solutions in financial markets.

Common charges for mobile phones and similar devices

The envisaged legislation for common charges for mobile phones and similar devices was announced in the 2020 European Commission work programme. It would propose to harmonise legislation on common chargers for mobile phones and similar devices. Its overall aim is to provide greater convenience and cost-savings for the consumer and reduce electronic waste. Due to the COVID crisis, this was postponed until 2021 and in February 2021, along with the New Circular Economy Action Plan, the Parliament called on the Commission to launch a common charger for smartphones and all small and medium-sized electronic devices.

New design requirements and consumer rights for electronics

This legislative initiative was announced in the Commission's 2021 work programme, A Europe fit for the digital age, and is due on Q2 2022. The Commission intends to propose measures on eco-design of mobile phones, tablets, computers, and computer servers are intended to be implemented in line with the Circular Economy Action Plan. The future e regulation for mobile phones and tablets will aim to address issues such as limited availability of the most damaged spare parts; limited availability of

updated versions of the operating system, firmware, or software; cost and ease of repair; and reduced battery endurance over time. Whereas the future regulation on computers and computer servers will aim to update energy efficiency requirements for these products, increase reparability of computers, improve lifetime of both computers and batteries, and reduce purchases of unnecessary chargers. Furthermore, the Commission has launched other initiatives to improve the sustainability of products, including electronics, such as the Digital Product Passports introduced by the Sustainable Products Initiative[10].

Multimodal digital mobility services

In September 2021, during the State of the Union letter of intent to the European Parliament President, Ursula von der Leyen and Maroš Šefčovič announced that the multimodal digital mobility services would be among the key new initiatives of the European Commission for 2022. The aim is to facilitate the planning and purchase of transportation tickets in the EU by implementing route-planners or ticket vendors to assist consumers by comparing travel options. The legislative proposal is planned to be presented by the Commission during the second quarter of 2022. However, in the Commission Work Programme 2022, this legislative proposal is announced for the fourth quarter of 2022.

1.3.4. Online services and e-commerce

EU VAT for e-commerce package (EU VOEC)

The EU VAT for e-commerce package is one of the priorities under the Digital Market Strategy and was first adopted by the Council in December 2017. Since then, it has been deployed gradually and has introduced reforms to the VAT requirements for business-to-consumer (B2C) ecommerce sellers and marketplaces. Furthermore, it aims to facilitate cross-border trade, ensure fair competition for businesses in the EU, and combat fraudulent VAT practices. It has also improved the mini one stop shop (MOSS) portal, which is a system to declare and pay VAT on B2C for certain services in the EU.

Payment Services Directive (EU) 2015/2366

The Payment Services Directive has been applied since January 2016, with Member States required to incorporate it into national law since 2018. The aim of this Directive is to improve existing EU regulation for electronic payments by considering emerging payment methods, such as through mobile or internet. It sets requirements to protect consumers' financial data, transparency for information requirements for payment services, and the rights and obligations of users and providers of these payment services. Furthermore, this Directive strengthens the role of the European Banking Authority (EBA) to develop a central register of authorised payment institutions, assist in resolving disputes, and develop regulatory technical standards.

e-Commerce Directive 2000/31/EC

The e-Commerce Directive entered into force in July 2000 with the deadline for transposition in Member States by January 2002. This Directive establishes a set of standardised rules at an EU-level on various key issues related to e-commerce. It covers several online services including news services,

[10] European Parliament, *Europe's Digital Decade and Autonomy*, 2021, available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/695465/IPOL_STU(2021)695465_EN.pdf.

advertising, professional services, and selling. Member State governments are obliged to ensure that online advertising identifies the following clearly: the advertising itself, the company or personal responsible, and promotional offers, games, or competitions along with their conditions.

Geo-Blocking Regulation (EU) 2018/302

The Geo-blocking Regulation aims to give all EU consumers equal rights to access a trader's goods or services, under the same terms, irrespective of their location. The new rules aim to tackle geo-blocking as well as other forms of discrimination based on nationality, residence or establishment. It applies in principle to both business-to-consumer (B2C) and to business-to-business (B2B) transactions.

Proposal for a Digital Services Act COM/2020/825

The proposal for a Digital Services Act is a legislative proposal by the European Commission that was submitted to the European Parliament and the European Council in December 2020. The objective of this proposal is to modernise the EU's legislative framework by updating the concepts contained in the e-Commerce Directive. The Digital Services Act proposal aims to create a safer digital space in which the fundamental rights of all users of digital services are protected. In particular, the proposal concerns online intermediaries and platforms such as online marketplaces, social networks, content-sharing platforms, app stores, and online travel and accommodation platforms.

Legislative proposal on a Single Market Emergency Instrument

This legislative proposal was first introduced in a speech delivered at the EU Industry Days in February 2021 by Ursula von der Leyen. This new instrument would aim to ensure the free movement of goods, services, and people, with greater transparency and coordination in times of crises. The key elements of the single market emergency instrument would be to reinforce single market governance tools and procedures, improve transparency and coordination on intra-EU export restrictions and services restriction. Furthermore, the legislative proposal would strengthen structures and tools to facilitate the circulation of goods and services in the context of border restrictions, target measures for speedier product availability, enhance market surveillance procedures, and reinforce cooperation and information-sharing in public procurement.

1.3.5. Data governance and management

Open Data Directive (EU) 2019/1024

The Open Data Directive was adopted in June 2019 and revises Directive 2003/98/EC on the re-use of public sector information (the PSI Directive). The aim of the Directive is to strengthen the EU's data-economy by increasing the amount of publicly held and funded data available for re-use. The Directive introduces an obligation for public bodies to publish available data unless access is restricted or excluded. It brings public undertakings such as public utilities under the PSI, and it proposes using Implementing Acts to set out lists of high value datasets which must be made available by public bodies.

General Data Protection Regulation (GDPR) (EU) 2016/679

The General Data Protection Regulation (GDPR) has applied since May 2018. The GDPR is a data privacy and security law that aims to allow EU citizens to better control their personal data by facilitating citizen access, providing an individual the right to know when their personal data has been hacked, and providing rules on the right to erasure of personal data from platforms. Additionally, it harmonises rules to reduce excessive bureaucracy and allow business to benefit from greater consumer trust. It also establishes the data protection officer role, which is responsible for data protection and is designated by public authorities and businesses which process data on a large scale.

Regulation on the free flow of non-personal data (EU) 2018/1807

The Regulation on the free flow of non-personal data has applied since June 2019. The aim of this Regulation is to ensure free movement of non-personal data across borders so that every organisation can store and process data anywhere in the EU. Furthermore, public authorities will retain access to data, even when it is in another EU country or when it is stored or processed in the cloud. It encourages providers to develop codes of conduct regarding the conditions under which users can move data between cloud service providers and back into their own IT environments.

Directive on certain aspects concerning contracts for the supply of digital content and digital services (EU) 2019/770

The Directive on certain aspects concerning contracts for the supply of digital content and digital services aims to fully harmonise a set of key rules that are so far not regulated at Union level. It includes rules on conformity of the digital content, remedies available to consumers in cases of lack of conformity of digital content with the contract and certain modalities for the exercise of those remedies. The Directive also aims to harmonise certain aspects concerning the right to terminate a long term contract, as well as certain aspects concerning the modification of the digital content.

Data Governance Act (DGA) COM(2020) 767

The Data Governance Act is a legislative proposal that was first announced within the 2020 European strategy for data and officially presented in November 2020. The aim is to foster the availability of data for use by increasing trust in data intermediaries and by strengthening data-sharing mechanisms across the EU. It would make public sector data available for safe reuse when such data is subject to rights of others. Furthermore, it creates a new business model to foster data intermediation services, to help companies or individuals share data in a secure way and allows for data use on altruistic grounds.

European Health Data Space

The European Health Data Space was first announced in the State of the Union address in September 2020 by European Commission President Ursula von der Leyen. The combined evaluation roadmap and inception impact assessment were published 23 December 2020 and a consultation ran from 3 May to 26 July 2021 and the legislative proposal is expected for 2022[11].

[11] European Parliament, Legislative Train Schedule, *Creation of A European Health Data Space*: https://www.europarl.europa.eu/legislative-train/theme-promoting-our-european-way-of-life/file-european-health-data-space/11-2021.

The aim is to promote safe patient data exchange, facilitate citizen control over their own health data, and support research on medicine treatments and outcomes. Furthermore, it encourages access to health data for policy making purposes and regulation, supports digital health services, and outlines the safety and liability aspects of artificial intelligence in health care. The legislative proposal resulting from this consultation is expected to be adopted in the fourth quarter of 2021.

Data Act

The Data Act was first announced in the 2020 European strategy for data and then its Inception Impact Assessment was published in May 2021. The adoption of the Data Act is expected by the first quarter of 2022. This proposal aims to create a safer digital space in which the fundamental rights of all users of digital services are protected. In particular, the proposal concerns online intermediaries and platforms such as online marketplaces, social networks, content-sharing platforms, app stores, and online travel and accommodation platforms. The DA will include a review of the rules of the legal protection of databases and deal with the planned revision of the Database Directive. In addition, the Trade Secrets Directive was discussed in the DA Inception Impact Assessment, which is an instrument that ensures protection against (un)lawful acquisition, use and disclosure of certain business sensitive information[12].

European Alliance for Industrial Data, Edge, and Cloud

The Alliance builds on the 2020 European data strategy and was endorsed by the European Council and the Declaration on European Cloud, signed by all Member States, in October 2020. This Alliance aims to bring together businesses, Member States representatives and relevant experts to strengthen the position of EU industry on cloud and edge technologies. Furthermore, it will serve the needs of EU businesses and public administrations that process sensitive categories of data and has the objective to increase Europe's leadership position on industrial data.

1.3.6. Copyrights and audio-visuals

Directive on Copyrights and related rights in the DSM Directive (EU) 2019/790

The Directive on Copyrights and related rights in the Digital Single Market (DSM) has applied since June 2019 and became law in all EU countries since June 2021. The Directive updates the EU's copyright legislation. It is composed of three over-arching objectives: adapt key exceptions to copyright in the digital and cross-border environment, improve licensing practices and facilitate wider access to content, and achieve a marketplace for copyright. It aims to make it easier to use copyright-protected material for some purposes, including access to knowledge. It also includes the protection of press publications for online use and provides rules for fair remuneration for authors and performers, among others.

[12] The directive can apply to (business sensitive) data. The assessment of the application of the directive in the context of the data economy is ongoing, and it includes the launch of a study focusing on four key sectors (automotive, health, energy and financial services). Based on this assessment, clarifying guidance may be issued at a later date.

Satellite and Cable Directive (EU) 2019/789

The Satellite and Cable Directive was first proposed by the European Commission in September 2016 in the context of the Digital Single Market strategy and along with a legislative package designed at the revision of EU copyright regulations. The objective of this Directive is to facilitate and promote cross-border delivery and access of online services to broadcasts. Furthermore, it aimed to adapt the EU legal framework to enable digital retransmissions over closed networks of TV and radio programs from other Member States.

Portability Regulation (EU) 2017/1128

The Portability Regulation has been applied since 2018 with the aim of ensuring that subscribers to an online content service in one Member State can access it when traveling cross-borders to other EU Member States. It calls for giving access in the same way as in their country of residence and includes video on demand, music streaming, and online game marketplaces. To note, there is no obligation to provide the same quality, unless it has been agreed with the subscriber. However, the quality for the service must not be deliberately reduced.

Radio Equipment Directive 2014/53/EU

The Radio Equipment Directive entered into force in June 2014 with the deadline for transposition into Member States by June 2016, repealing Directive 1999/5/EC. The aim of the Directive was to harmonise the laws of Member States related putting radio equipment on EU's internal market and applies to all equipment which emits or receives radio waves for radiodetermination or communication purposes. It sets rules to ensure that radio equipment devices respect health and safety requirements and sets out means for market surveillance to track products which fail to comply with requirements.

Database Directive 96/9/EC
[under revision]

The Database Directive, which was adopted in March 1996, aims at supporting the development of the European database industry. In accordance to the Directive, all databases that *'constitute the author's own intellectual creation shall be protected as such by copyright'*. The European Commission conducted an evaluation and carried out a consultation in 2017 and 2018 to understand how such directive, and in particular the *sui generis* protection of databases, is applied and what impact it had on users and makers. The second evaluation of the Directive from 2018 showed that, while the Database Directive provides added value, it could be revisited to facilitate data access and use. The Commission work programme for 2021 foresees the review of the Database Directive in Q3 2021.

1.3.7. e-Government

E-invoicing Directive (EU) 2014/55

The E-invoicing Directive entered into force in May 2015 with November 2018 as the deadline for transposition into the Member States. This Directive was adopted in tandem with laws on public procurement to result in a greater uptake across Europe of e-voicing by contactors for work in the public sector. This does not apply to contracts that fall within the scope of Directive 2009/81/EC in sectors such as defence and security.

Electronic identification rules - eIDAS Regulation (EU) No 910/2014 [under revision]

The eIDAS (electronic identification, authentication and trust services) Regulation entered into force in September 2014 and has applied since July 2016. It provides a predictable regulatory environment to enable secure and seamless electronic interactions between businesses, citizens, and public authorities. It ensures that people and businesses can use their own national electronic identification schemes (eIDs) to access public services in other EU countries where eIDs are available. The eIDAS Regulation creates a European internal market for electronic trust services by ensuring that they will work across borders and have the same legal status as traditional paper-based processes.

Digitalisation of visa procedures

The envisaged legislation for the digitalisation of visa procedures was announced in the 2021 European Commission work programme and proposes to fully digitalise the visa procedure by 2025 developing a digital visa and the implementing the ability to submit visa applications online. The legislative proposal is scheduled to be published in the fourth quarter of 2021.

2. DATA PROTECTION AND GOVERNANCE

The interplay between the items in this area is analysed along three dimensions:

- The distinction between personal and non-personal data;
- The conditions of the parties involved; and
- Interaction between an open data approach and data protection regimes.

2.1. Personal and non-personal data

While the GDPR only applies to personal data[13], in the Free Flow Regulation on non-personal data, the EU also recognises that non-personal data are a source of potential great value in the context of the development of AI, IoT and other emerging technologies, and for the platform economy more broadly defined. There is awareness of the existence of mixed datasets with personal and non-personal data that can be inextricably linked. This requires considering both anonymisation and re-identification of data and their implications in the applicable regime. Therefore, legal acts on data may be applied concurrently to different scenarios and actors. A simple classification based on the dualism of personal data/non-personal data provides a first map of interactions among legal acts within the policy area of data governance and management.

2.1.1. Personal data

The EU has put in place a solid legal framework for the protection of personal data that fundamentally pivots on the GDPR, and the ePrivacy Directive. The latter is being revised both for taking into consideration new technological development and for better alignment with the GDPR. The complementarity between the GDPR and the ePrivacy Directive is recognised and guaranteed in Article 95 of the GDPR, which prevents from imposing additional obligations on natural or legal persons that are already subject to specific obligations with similar objectives set out in the ePrivacy Directive. The ePrivacy Directive would be repealed by the proposed ePrivacy Regulation[14]. The complementarity with the GDPR is acknowledged in Article 1.3 of the ePrivacy Regulation by stating that the aim of the Regulation is to complement the GDPR by defining rules for the purposes of protecting fundamental rights and freedoms of natural and legal persons in the provision and use of electronic communications services. In particular, it protects the rights to respect private life and communications and the protection of natural persons with regard to the processing of personal data. It also ensures free movement of electronic communications data and services within the Union (Article 1.3 GDPR).

2.1.2. Non-personal data

The Free Flow Regulation is solely focused on non-personal data[15]. Hence, the GDPR and the Free Flow Regulation of non-personal data jointly provide for the free movement of 'all' data within the EU.

The Free Flow Regulation lays down a general prohibition against data localisation requirement (Art. 4.1) unless justified on grounds of public security, whereas the GDPR allows the free movement of

[13] Article 4.1. GDPR: 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

[14] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications).

[15] Article 1 of the Regulation defines the subject matter: "This Regulation aims to ensure the free flow of data other than personal data within the Union by laying down rules relating to data localisation requirements, the availability of data to competent authorities and the porting of data for professional users".

personal data within the Union without restrictions on the grounds of protection of personal data (Art.1.3). Thus, the complementarity between the GDPR and the Free Flow Regulation on free movement of data within the Union and data portability is smooth, to the extent that the classification of data (as either personal or non-personal) is evident and unquestioned. Mixed datasets, especially with linked personal and non-personal data, use anonymisation and re-identification mechanisms and require closer consideration to provide a suited solution.

2.1.3. Personal and non-personal data

The Open Data Directive and the Data Governance Act focus indistinctively on both personal and non-personal data. Personal data are defined in conformity with the GDPR. The proposed Data Governance Act complements the Open Data Directive as its scope of application covers those data held by public sector bodies that, being subject to rights of others, fall outside the scope of the Open Data Directive. As per Article 3 of the Data Governance Act, the text applies to data held by public sector bodies which are protected on certain grounds: commercial and statistical confidentiality, intellectual property rights, or personal data. While Article 1.2 of the Open Data Directive excludes, from its scope of application, documents for which third parties hold intellectual property rights, documents excluded from access on grounds of commercial confidentiality, statistical confidentiality (Article 1.2.d), and documents that cannot be accessed on grounds of personal data protection (Article 1.2.h). The adoption of the proposed Data Governance Act would then fill a regulatory gap that the material scope of the Open Data Directive had left unaddressed. Concurrently, the Open Data Directive in combination with the Data Governance Act would pave the path towards an open data environment, facilitating data sharing with an important role of data sharing intermediaries and under the FAIR data principles (Findability, Accessibility, Interoperability, Reusability). In addition, the proposed Data Act would complement a legal framework conducive to a fair allocation of data value among actors of the data economy, especially B2B (data sharing, portability, safeguards of non-personal data in international contexts), as further discussed below.

2.1.4. Mixed datasets and prevalence of personal data protection

Datasets, in practice, are frequently mixing personal and non-personal data; moreover, the processes for anonymising or re-identifying data can change the status of the data at different stages throughout their life cycle. It is, thus, important to analyse how personal data and non-personal data regimes interact in mixed datasets and, in particular, when data are so inextricably linked that separation is not feasible, affordable, or commercially reasonable. As the Guidance on the Free Flow Regulation[16] explains, the key rule is to apply each regime to the respective type of data, and in case that separation or identification is not possible ('inextricably linked'), personal data protection prevails. This proposal is based on the following reasons and legal grounds. First, Article 2.2 Free Flow Regulation provides that:

> 'In the case of a dataset composed of both personal and non-personal data, this Regulation applies to the non-personal data part of the dataset. Where personal and non-personal data in a dataset are inextricably linked, this Regulation shall not prejudice the application of Regulation (EU) 2016/679.'

[16] See the Practical guidance for businesses on how to process mixed datasets available at: https://digital-strategy.ec.europa.eu/en/library/practical-guidance-businesses-how-process-mixed-datasets.

This means that, in a case of a mixed dataset, the Free Flow of Non-Personal Data Regulation applies to the non-personal data part of the dataset, while the GDPR's free flow provision (Art. 1.3 GDPR)[17] applies to the personal data part of the dataset. If the non-personal data parts and the personal data parts are 'inextricably linked', the data protection rights and obligations stemming from the GDPR fully apply to the whole mixed dataset, even when personal data represent only a small part of the dataset. The presence of personal data, irrespective of how relevant or significant the part is in the context of the whole set, triggers the protection for personal data[18]. This interpretation is in line with the right to personal data protection guaranteed by the Charter of Fundamental Rights of the European Union.

Consequently, in the interplay between all data-related legal acts, it is confirmed that those provisions facilitating access to data and re-use would apply without prejudice of the protection of individuals regarding the use of personal data under Union and national law, particularly GDPR and any supplementing provisions of national law (Art. 1.4 Open Data Directive). This explains, for instance, that in promoting use and re-use of open data, the costs of anonymisation of documents can be considered in the charging of fees and the allowed recovery of marginal costs (Art. 6 Open Data Directive). While rendering information anonymous is intended to reconcile the public interest in making public sector information as re-usable as possible with the obligations under data protection law, it does entails costs. Under the Data Governance Act, which covers data protected on grounds of personal data protection, it is particularly relevant to consider the implementation (Recital 6) of techniques enabling privacy-friendly approaches to databases that contain personal data. This includes techniques such as anonymisation, pseudonymisation, differential privacy, generalisation, or suppression and randomisation. 'In many cases this implies that the data use and re-use in this context can only be done in a secure processing environment set in place and supervised by the public sector' (Recital 6). Furthermore, the Data Governance Act reaffirms that, in general, the processing of personal data should rely upon one or more of the grounds for processing provided in Article 6 GDPR. A more speculative appraisal of the DGA effects is added in the text box below.

[17] Article 1.3 GDPR: The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

[18] Commission Staff Working Document, Impact Assessment accompanying the document Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union (SWD(2017) 304 final), part 1/2, p. 3.

Box 1: The DGA and international data transfer

The DGA also establishes specific conditions applying to international transfers of certain categories of non-personal data, identified as 'highly sensitive' (Article 11 and Recital 19). This kind of data should be identified by subsequent Union law, for instance in the context of the European Health Data Space proposal. In this respect it has been observed that the DGA might render such international transfers difficult (Baloup, 2021). It might also compound further the problems with international transfer of data after that the US Safe Harbour and later the EU-US Privacy Shield were invalidated by the Court of Justice (Schrems I and II case-law, C-362/14 and C-311/18), as illustrated by Kiner (2020). Such problems have so far created legal uncertainty to the detriment of companies dealing with EU-US data transfers that may result in soft data localization (Chander, 2020). An econometrics study commissioned by Digital Europe shows that, reversing the current trends and harnessing the power of international data transfers, Europe could be €2 trillion better off and gain two million jobs by the end of the Digital Decade (Digital Europe, 2021). It is yet premature to conclude that the DGA will exacerbate such problems, but this is an example of how lack of coherence between legal acts and the difficult trade-off between protecting citizens and not hampering businesses can be detrimental to the European data economy and to the renewed partnership with the US.

2.2. On the conditions of the parties: B2C, B2B, B2G, and G2B

The legal acts on data can also be classified on grounds of the condition that the parties to the legal provisions on data access, use and re-use, or data sharing are addressed to. Essentially, the GDPR focuses on the protection of natural persons regarding the processing of personal data and the free movement of personal data ('data subject'). Other data-related legal acts provide rules governing data access, data use and re-use, or data sharing in the context of B2B or B2G relations. This is particularly visible in the Data Governance Act and the Open Data Directive, whose material scopes of application are defined by the fact that data (or documents) are held by public sector bodies or public undertakings. In such cases, the 'G' component of the relation (G2B) is consubstantial to the goal of ensuring the social benefit of protected public sector data. The Data Governance Data also addresses B2B and B2C data sharing with the establishment of a notification scheme for the provision of data sharing services. Thus, in Chapter III (Arts. 9 and following), the Data Governance Act sets out the requirements that providers of certain data sharing services are subject to: intermediation services between data holders that are legal persons and potential data users; between data subjects seeking to make their personal data available to potential data users; and members of a data cooperative (data subjects, one-person companies, micro-SMEs). The Free Flow Regulation tackles the portability of data in B2B scenarios while the GDPR provides rules for data portability that benefit the data subject (natural persons). The proposed Data Act intends to complement the existing framework and enhance access to, and further use of data in the benefit of both public and private actors. So far, the conditions of access and further usage of data in B2B contexts are frequently agreed by contracts between the parties. In the negotiation and conclusion of such agreements, unfair situations due to asymmetric bargaining of powers between the parties, or restrictive competition practices may emerge. Therefore, the proposed Data Act aims to provide fairness, clarity, and certainty with respect to B2B access and sharing of data, both personal and non-personal, and to facilitate the use of privately held data by the public sector. The Data Act is also expected to deal with the revision of the Database directive, but at the time of writing only the roadmap and inception impact assessment were published, which are not sufficient for a thorough legal scrutiny.

As noted by the High-Level Expert Group on Business-to-Government (B2G) data sharing[19], there are some obstacles in B2G data use and data sharing to serve the public interest that requires attention. An effective access to data for public interest depends on organizational, operational, technical, cultural, and legal factors. Lack of infrastructures, models and data sharing culture for public interest compromises the effectiveness of B2G data sharing. A delicate balance is needed between the protection of sensitive business data and possibility for data providers to continue monetizing their data, and the fluent access to data for serving public interest. Although there are some references in the Trade Secret Directive to public interest (Arts. 1.2.b[20], 5.b, 11.2.g, 13.1.g) as a limitative or exclusion factor as well as, *inter alia,* in the Database Directive (Art. 9.c referring solely to public security or administrative and judicial procedure that is narrower than the idea of serving the public interest). However, these do not suffice to provide a clear, consistent, and comprehensive framework for B2G data sharing. Likewise, in addition to existing sectoral rules[21], data sharing in B2B contexts may require further facilitating rules. First, to promote contractual fairness in private agreements to regulate B2B data sharing in asymmetric situations. Second, to ensure that access and use of co-generated non-personal data, especially machine-generated data and linked to the use of IoT, AI and other emerging technologies, does not create unfair competition problems. Even more, it might be considered whether a sector-specific approach to B2B data sharing, after the accrued experience and the lessons learned in the application of existing sectoral rules, is the optimal model, or, on the contrary, has a gap to fill with a horizontal, coherent B2B data sharing regulatory strategy. Thus, the proposed Data Act would fill the gaps identified in B2B data sharing to ensure fairness in market transactions and in B2G contexts to facilitate the use of data for public interest.

2.3. On the interaction between data access and data protection

The third vector to approach data-related legal acts underlines the interplay, and critical balance between data governance and open data policies that promote data access, use and re-use, and the protection regimes that exclude or restrict access to data on grounds of confidentiality, trade secrets, intellectual property rights, and privacy. From this perspective, the complementarity between the proposed Data Governance Act and the Open Data Act is easily identified. As the latter excludes from the scope of application precisely these documents (data) on grounds of such protection schemes, the Data Governance Act would come to fill that gap. As the proposal explains, certain categories of data in public databases are often not made available, not even for research or innovative activities.

---

[19] Towards a European strategy on business-to-government data sharing for the public interest *Final report prepared by the High-Level Expert Group on Business-to-Government Data Sharing*, European Union, 2020.

[20] Article 1.2.b Trade Secret Directive: *(b) the application of Union or national rules requiring trade secret holders to disclose, for reasons of public interest, information, including trade secrets, to the public or to administrative or judicial authorities for the performance of the duties of those authorities.*

[21] Inter alia, bank account information via the Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/ EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ L 337, 23.12.2015, pp. 35-127); metering and electricity consumption information via the (future) directive on common rules for the internal market in electricity (COM(2016)864/F2); repair and maintenance information via Regulation (EU) 2015/758 of the European Parliament and of the Council of 29 April 2015 concerning type-approval requirements for the deployment of the eCall in-vehicle system based on the 112 service and amending Directive 2007/46/EC (OJ L 123, 19.5.2015, pp. 77-89).: information on medicinal products and clinical trials via the Commission Regulation (EC) No 729/2004 of 15 April 2004 concerning the classification of certain goods in the combined nomenclature; chemical properties of substances via the Regulation (EC) No 1907/2006 of the European Parliament and of the Council of 18 December 2006 concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH), establishing a European Chemicals Agency, amending Directive 1999/45/EC and repealing Council Regulation (EEC) No 793/93 and Commission Regulation (EC) No 1488/94 as well as Council Directive 76/769/EEC and Commission Directives 91/155/EEC, 93/67/EEC, 93/105/EC and 2000/21/EC.

These categories include commercially confidential data, data subject to statistical confidentiality, data protected by intellectual property rights of third parties, including trade secrets and personal data not accessible because of specific national or Union legislation, such as GDPR and ePrivacy Directive. The required implementation of costly and time-consuming protection measures to comply with relevant legal conditions for each category of data has led to the underutilisation of such data. The proposed Data Governance Act responds to this need and fills the gap for data held by public sector bodies. The interplay is also recognised in the GDPR as a natural limit in the exercise of the right of access to personal data by the data subjects, provided that the protection of third parties' rights does not entail in practice a total rejection (Recital 63). A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, to be aware of, and verify, the lawfulness of the processing. 'That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject'. Therefore, the consistency of the right of access to personal data that underpins the GDPR, and the protection of certain rights should be preserved to the maximum extent possible with the red line drawn to prevent a total refusal of the right of the data subject. Yet, there is an interesting interplay between the *sui generis* protection provided for by the Database Directive and the data-driven innovation policy in the context of technological advances. In the current legislative scenario, datasets can be protected as a trade secret if relevant protection conditions are met (Art. 2.1 Trade Secret Directive), by intellectual property rights if they are original (Art. 3 Database Directive). They can also be protected under the *sui generis* protection for databases (even if they are not original) on grounds of the substantial investment in the obtaining, verification of presentation of contents to prevent extraction and/or re-utilization of the whole or of a substantial part of that database (Art. 7.1). In a pre-digital context, these protection schemes fit together and provide a coherent framework. The characteristics of the data economy and the need to foster data-driven innovation require a re-evaluation of the existing framework. The policy aspiration to facilitate data access, further use, and free flow might be countered by existing protection schemes that lead *de facto* to restrictions in the access to and the further use of valuable data linked to IoT, AI and other emerging technologies. Such an undesired effect does not result from a regulatory gap as such, as long as there are rules potentially or inadvertently addressing the issue. It might be considered instead as an overlap or a supervening conflict between existing rules and policy goals in the database industry and emerging data-economy policies. In that regard, the gap would be filled, or the conflict untangled with the review of the Database Directive and the clarification of the controversial points. Primarily, the critical points are the following. First, the unclear status of machine-generated data and IoT data under the *sui generis* database right. Machine-generated data can be massive and of utmost importance either for public interest or for private activities. Therefore, the interpretation of the Database Directive provisions in the current drafting or a future review of the Directive to address this controversy is critical to assess whether the *sui generis* protection is consistent with the data policy in the Union or, on the contrary, is counterproductive as it represents an obstacle to data access. Second, is the distinction between collecting and systematizing tasks (traditional database making) and data creation activities (updating, maintenance, publication, curation). The original goal of the Database Directive to promote investment may become a disincentive and a barrier for the data economy depending on the interpretation of the extent and scope of database making or the final direction taken in the review of the Directive regarding data creation activities. In addition to the legal analysis presented so far, some final more general considerations are reported in the text box below.

Box 2: On B2G data sharing also as a matter of non-regulatory governance

The access by governments to private sector data, or B2G data sharing is a particularly wicked issue. The Commission Data Strategy (European Commission, 2020b: pp. 7-8), considers the insufficient access by public bodies to private sector data as a main barrier to improve evidence-driven policy-making and public services provisions. There often are conflicts of interests between the private and the public actor, for the latter aims at creating public value rather than mere financial gains that tend to be sought by the former. The lack of governance frameworks creates uncertainties for companies sharing data as to issue of 'liability regimes, intellectual property, and competition law', as well as problems related to privacy and the protection of customers' personal data (Micheli, 2020, p.2). Furthermore, there are economic barriers: monopolistic companies charging high prices, high transaction costs and perceived risks for data providers, and lack of incentives for private companies (Martens and Dutch-Brown, 2020). So, there is a clear power dimension that relates to data governance, defined as the power relations between all the actors affected by, or influencing, the way data are accessed, controlled, shared, and used, the various socio-technical arrangements set in place to generate value from data, and how such value is redistributed between actors. In this context, data governance does not refer to data management practices, but to the decisions made over data, who is able to make such decisions and thus to influence the way data are accessed, controlled, used, and benefited from (Abraham et al., 2019). So, data persistence contributes to blur the understanding of the potential risks and benefits of sharing own data with government. Prior beliefs together with heuristics and bias may over-inflate perceived risk or expectation about fairness, reciprocity, and equity, especially for non-dominant private sector actors.

3. DIGITAL SERVICES AND MARKETS

3.1. The role of intermediaries and the interplay between digital services and markets acts with data governance

In the data economy, platforms and other providers of intermediary services are principal actors. They facilitate matching, reduce transaction costs, render trade more efficient, and help businesses reach their customers and explore new markets. Their prominent position in the market is built on data and fuelled by strong data-driven indirect network effects (Recital 2 P2B Regulation). Data generated through or in relation to platforms foster innovation, and assist firms in business intelligence, product development, and process optimization. Data provide valuable, deep insights on how markets function, prospects, and trends. However, different actors – platform operator, professional/business users, consumer users, third parties - have interests in getting access to data and opportunities to re-use it and, therefore, conflicting interests may concur in the elaboration and the implementation of data-related practices in the platform economy. Data asymmetries and the power of data aggregation (whose replication is unfeasible or unaffordable) reinforce the dominant position of platforms and the economic dependence of users, even professional/business users. This finding captures the critical interplay between the data governance and management policy area and the legal acts on digital services and digital markets (namely, e-Commerce Directive, P2B Regulation, DSA, DMA).

In the context of the platform economy, data sharing, access, and usage can be internal (in platform), between users and the platform operator, which collects, observes, and infers data from users' activity, or external, in relation to third parties, either competitors or data seekers, or even public sector bodies and authorities. There are different incentives or disincentives for the platform to share data internally or externally. Internally, platforms' terms and conditions and policies establish the conditions on which users get access to, are entitled to use, and must provide data. Therefore, data practices in the platform economy must be confronted with the data principles and rules provisioned in the data-related legal acts. The e-Commerce Directive laid the foundations for the provisions of digital services (information society services) in the Union. The extraordinary expansion of the market and the sophistication of the business models required first some sector-specific provisions (i.e., in the Audio-Visual Services Directive; the Copyright Directive) and subsequently a more ambitious initiative to revisit and update the legal framework with the proposed DSA. Furthermore, it required, to a certain extent and for certain platforms with gatekeeping potential, the proposed DMA. In the e-Commerce Directive, the interplay with data-related acts, in force at that time, is assumed with a simple and clear recognition of compatibility (Recital 14). It is stated that personal data protection and privacy rules are fully applicable to information society services; and therefore, it was not needed to cover this issue in the Directive to ensure the smooth functioning of the internal market, in particular the free movement of personal data between Member States. Accordingly, the implementation and application of the e-Commerce Directive had to be made in full compliance with the principles relating to the protection of personal data, as regards to unsolicited commercial communication and the liability of intermediaries. Finally, in the same Recital, it is explicitly recognised that it is not aimed to prevent the anonymous use of open networks such as the Internet. The relevance that access to personal data gained in the decades following the adoption of the e-Commerce Directive, explains the more explicit and wide treatment of data-related issues in the subsequent legal acts and initiatives. The key points of interaction between the P2B Regulation, the DSA and the DMA, and the data legal framework are considered below.

3.2. Data-related issues in the P2B Regulation

The scope of P2B Regulation application is limited to the (contractual) relationship (Art. 2.2.c) between business users (Art. 2.1) and certain intermediaries (Art. 1.1) as defined by the Regulation (P2B relationship): online intermediation services (Art. 2.2) and online search engines (Art. 2.5). This scope of application is narrower than the proposed scope of the DSA and, therefore, the interplay between the P2B Regulation, as *lex specialis,* and the DSA must be considered. Within its scope of application as defined above, the P2B Regulation contains several provisions on data-related aspects. The starting point is the declaration that if personal data are processed in the platform, the GDPR, the ePrivacy Directive and any other relevant legislation must be complied with. Hence, the natural interplay with personal data legislation is recognised. Beyond that, it must be taken into consideration that the relationship between the provider and the professional user is based on a contractual agreement (including terms and conditions and internal policies included by reference). These contractual terms will address and govern data access, data use and data sharing within the platform.

The P2B Regulation aims to ensure fairness and transparency in these P2B relationships by limiting certain clauses, requiring transparency obligations, or imposing duties. As far as data are concerned, there are two key provisions. First, Article 4 on restriction, suspension, and termination. Second, Article 9 on access to data. When a provider decides, in conformity with the terms and conditions and its internal policies, to restrict, suspend or terminate the provision of the services to a given business user a statement of reasons for that decision must be provided. Against this decision, the professional user can complain (by the complaint-handling mechanisms of Art. 11). In case that the decision is revoked accordingly, the provider must reinstate the business user and provide him/her with any access to personal and non-personal data resulting from its use of the services, up to the moment the decision (of restriction, suspension, or termination) took effect. Therefore, the Regulation establishes here an obligation to provide or restore access to data. As per Article 9, which clearly address the data access question, the Regulation imposes a transparency obligation on providers regarding the technical and contractual conditions to access data by the business user. Data refer to both personal and non-personal data. The description of data access policies (or non-access to data at all) must be contained in the terms and conditions (including the items listed in Art. 9.2). It is important to note here two considerations. Firstly, that this provision does not prejudice the application of GDPR and the ePrivacy Directive, and any other relevant legislation, to such data. Secondly, that this provision only concerns a duty of transparency, but it does not entail any obligation on the provider to disseminate or not personal or non-personal data to business users (Recital 35). This leads to two conclusions. The interplay between the P2B Regulation and the data protection legislation as far as personal data and privacy legal acts are concerned, is preserved and unaltered. In fact, the Regulation aims to complement rules on data access and use with specific provisions in B2B contexts. From this perspective, the P2B Regulation may create a regulatory gap, which is two-fold. First, there is no obligation to share data or provide access to, but a mere duty to disclose it in the terms and conditions. So, there is no duty beyond that. It is naturally not a gap if it embodies a policy decision. But it is interesting to connect it with the following point, insofar as a gap might appear if such transparency obligation is not applicable to similar services under equivalent policy conditions. Indeed, second, the rules provided for the Regulation, as limited as they have been described, apply solely to the services falling under the scope of the regulation. The P2B Regulation leaves services unregulated and data aspects unaddressed. And in the analysis of the interplay between the DSA and the P2B Regulation, this may represent regulatory gaps for consideration.

3.3. Data-related issues in the DSA

This paragraph is focused on the interaction between the DSA and the data protection and governance policy area. First, the compatibility with personal data and privacy protection is explicitly recognised (Article 1.5). Additionally, in several provisions regulating transparency and reporting obligations on hosting services providers (including online platforms), the inclusion of personal data in publicly accessible information is prohibited (i.e., Art. 15.4 or 30 DSA). Based on this key principle, the most interesting, and probably challenging interplay between the DSA and the data domain is in relation to solutions adopted to minimize the information asymmetry between the market players (platforms and very large platforms) and the regulators and authorities as the main addressees and beneficiaries. Many obligations and requirements provided for by the DSA are intended to ensure data accessibility for monitoring and compliance assessment purposes. There are also other addressees of data such as auditors (Art. 28) or vetted researchers (Art. 31). This scheme the DSA is built on is highly dependent upon a solid, well-defined, and fluent infrastructure to facilitate data access with such purposes. The need to specify the data to be provided to comply with the different obligations (risk assessment, audits, transparency reports, etc) should not be technically deemed as a regulatory gap, but it may be highlighted as an implementation need.

3.4. Data obligations in the DMA

The DMA crystallizes an *ex-ante* regulatory strategy aimed to ensure contestability of digital markets across the Union and to prevent unfair practices in the digital sector, where certain actors operate as 'gatekeepers' by complementing and reinforcing antitrust mechanisms. The prominent position of certain core platform service providers (Art. 2) and their gatekeeping potential to access markets, resources, services, or infrastructures have defied the competition law logic. As a matter of fact, competition law would be arguably too slow and to a certain extent inefficient. Therefore, the DMA represents a regulatory shift towards a pre-emptive model. As in other legal acts, the compatibility of the proposal with personal data protection framework is explicitly recognised. Not only the provisions of the DMA are applied without prejudice of the GDPR and other relevant legislation, but also the gatekeepers shall comply with and implement the obligations (under Arts 5 and 6) in compliance with the GDPR and, it must be added here, with the cybersecurity legislation, with consumer protections laws and with product safety legislation. Furthermore, in relation to certain obligations, the gatekeeper should enable business users to comply with GDPR requirements, for instance, with the obtaining of the consent when required (Art. 6.1.h), Recital 55). It is important to note, however, that the DMA is intended to complement the data protection laws. Transparency obligations on deep consumer profiling would help inform GDPR enforcement, and mandatory opt-out for data combination would supplement the existing level of protection under the GDPR. These statements in the Explanatory Memorandum contained in the Proposal for the Regulation COM(2020) 842 final (pp. 1-13)[22] spotlight the expected added protection that, beyond relying on and respecting existing data protection legislation, the DMA may bring. Within its scope of application delineated by the concept of gatekeeper, the DMA contains several data-related provisions that reveal an interplay with data protection legal acts. Article 5 contains a list of obligations that will follow the designation of a provider as gatekeeper and in respect of the core platform services. Letter a) prohibits the practice of combining

[22] See: https://ec.europa.eu/info/sites/default/files/proposal-regulation-single-market-digital-services-digital-services-act_en.pdf

personal data sourced from the core platform services with personal data from any other services offered by the gatekeeper or with personal data from third-party services, and of signing in end users to other services of the gatekeeper to combine personal data, unless the end user has been presented with the specific choice and provided consent in the sense of the GDPR. Article 6 lists obligations that are susceptible of being further specified. Without being a real gap, however, it has been questioned whether placing such obligations under Article 6 is appropriate or rather placing them under Article 5, where no further specification is needed. Specifically, the proposal has been made in relation to obligations under h) and i) that are data related. Attention will be solely focused on the former one due to its interactions with other legal acts. Letter h) describes an important obligation of portability of data for business users and end users. Portability of data is a clear intersection between GDPR for personal data, Free Flow Regulation for non-personal data and the DMA. The contribution of DMA to the portability regimes, where gatekeepers are obliged to it, should ensure that business users and end users can port that data in real time effectively, such as, for example, through high-quality application programming interfaces. In that sense, the portability is not approached as one-shot action, but as a continuous, dynamic process based on real-time solutions. It has been proposed whether it should be understood as a real portability right or rather as a 'right to continuous, real-time access to data in situ'. In assessing whether the adoption of the DMA fills or opens regulatory gaps, the following considerations must be made. First, it has been argued that the scope of application defined by an exhaustive list (despite the review mechanism of Art. 17) in Article 22 might neither be complete nor future-proof. The DMA applies to 'core platform services' defined as any of the following digital services: online intermediation services, online search engines, online social networking services, video-sharing platform services, number-independent interpersonal communication services, operating services, cloud computing services, advertising services. Only these services qualify. It is not a gap to fill if that represents an explicit choice. Second, the specification and the implementation of the obligations under Article 5 and, especially, under Article 6 will require further efforts to provide guidance and standards for compliance. That is not necessarily a regulatory gap, but it places the focus on the implementation stage. The solution can be adopted on a case-by-case basis along the logic of the DMA of dialogue authority-provider, or in form of Guidelines as the ones adopted under the P2B Regulation on rankings[23].

3.5. Digital services and digital markets

The interplay between the policy areas of consumer protection and competition and online services and e-commerce primarily crystallizes in the interaction among the e-Commerce Directive, the DSA, the P2B Regulation, and the DMA. All these legal acts together, in addition to certain provisions in sector-specific acts (Audio-Visual Services Directive 2010 and Copyright Directive 2019), shape the in-progress platform regulation in the Union. Whereas the DSA builds on the foundations of the e-Commerce Directive, the DMA builds on the P2B Regulation without conflicting with it. Concurrently, the DSA is a horizontal initiative that interweaves with the DMA but also with different policy goals and objectives. An enticing interplay to explore is whether the criteria (Art. 25 DSA) to define very large platforms for the purposes of the DSA – methodology to be set out in delegated acts – will be or should be consistent with the criteria for the designation of gatekeepers under the DMA or if these respective

[23] Guidelines on ranking transparency pursuant to Regulation (EU) 2019/1150 of the European Parliament and of the Council (OJ C 424, 8.12.2020, p. 1).

designations will have any mutual implications. Under the DSA, very large platforms, pursuant to a staggered scheme of obligations, are subjected to additional substantive obligations.

In the DMA, the designation as gatekeepers is linked to certain obligations stated (Art. 5 DMA) or to be specified (Art. 6 DMA). The interplay between the DMA and the P2B Regulation is of a complementarity nature. The DMA relies on concepts, definitions, and certain solutions (i.e., the Guidelines on rankings) of the P2B Regulation but differ in several aspects. First, even if the P2B Regulation excludes providers that are small enterprises pursuant to the Annex to Recommendation 2003/361/EC from certain obligations (i.e., Art. 11.5, Art. 12.7), the Regulation is not based on the size or the market relevance of the provider, whereas the logic of the DMA is to identify and designate on quantitative and qualitative criteria providers with gatekeeping potential. Second, while the P2B Regulation applies to online intermediation services and online search engines, the DMA covers online intermediation services, online search engines, online social networking services, video-sharing platform services, number-independent interpersonal communication services, operating services, cloud computing services, advertising services. From this comparison, there is a possible gap to highlight. The P2B Regulation restricts its scope of application to platforms (online intermediation services providers) that enable the initiation or the completion of B2C transactions. But it should be considered whether there are sound reasons not to extend the Regulation to platforms enabling B2B transactions.

4. ARTIFICIAL INTELLIGENCE

4.1. Concept and definition of AI in the legal acts

In assessing the status of the regulation on AI in the EU and selecting relevant the vertical legislative act that mention AI and are, thus relevant, the first step to take is to define the subject matter. AI is a multifaceted phenomenon whose operation depends upon a conjunction of actors (operators, users, manufacturers, data providers, distributors, etc.), components, and technological solutions, and with uses and purposes extremely varied and diverse. Therefore, a complete regulatory framework for AI will come as a combination of both AI-specific and general rules dealing with transversal aspects (data, cybersecurity, consumer protection, competition, IP rights, etc.). Legal acts defining and explicitly addressing AI systems

In this category there is basically only one legislative proposal presented by the Commission: the AI Act proposal[24]. Of relevance, however, there is also the European Parliament Resolution with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)) that includes a Proposal for a Regulation of the European Parliament and the Council on liability for the operation of Artificial Intelligence-systems. This is only and approved resolution that, however, contains an example of an AI-specific legislative proposal. We refer to it henceforth simply as Resolution on liability. The Resolution on liability act provides for rules on the placing on the market, the putting into service and the use of AI systems. The definition of AI system for the purposes of the proposed instrument is as follows: 'artificial intelligence system' (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with' (Art. 3.1 AI Act). The compromise text unveiled at the end of November 2021 by the Slovenian Presidency of the European Council ['Joint Compromise', Council of the European Union, Presidency compromise text, 29 November 2021, 2021/0106(COD), henceforth simply 'Joint Compromise'] proposed the changes to this definition as depicted in the screenshot below. The text, in its preamble, explains that the changes make an explicit reference to the fact that AI system should be capable of determining how to achieve a given set of human defined objectives by learning, reasoning, or modelling, to distinguish them of more traditional software systems, which should not fall under the scope of application of this proposed regulation.

[24] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts, COM (2021) 206 final, Brussels, 21.4.2021.

Figure 1: Changes to AI Act Definition introduced on 29 November 2021

Article 3
Definitions

For the purpose of this Regulation, the following definitions apply:

~~(1) 'artificial intelligence system' (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with;~~

'artificial intelligence system' (AI system) means a system that

(i) receives machine and/or human-based data and inputs,

(ii) infers how to achieve a given set of human-defined objectives using learning, reasoning or modelling implemented with the techniques and approaches listed in Annex I, and

(iii) generates outputs in the form of content (generative AI systems), predictions, recommendations or decisions, which influence the environments it interacts with;

(2) 'provider' means a natural or legal person, public authority, agency or other body that develops an AI system or that has an AI system developed **and places that system on the market or puts it into service** ~~with a view to placing it on the market or putting it into service~~ under its own name or trademark, whether for payment or free of charge;

(3) 'small-scale provider' means a provider that is a micro or small enterprise within the meaning of Commission Recommendation 2003/361/EC[31];

(4) 'user' means any natural or legal person, public authority, agency or other body using an AI system under its authority~~, except where the AI system is used in the course of a personal non-professional activity~~;

Source: European Council Interinstitutional file 2021/0106(COD)[25], page 3.

Nonetheless, since AI systems are defined as software with certain purposes and characteristics, software-related rules may still be relevant to them. Likewise, insofar as AI systems' outputs are content, predictions, recommendations, or decisions, legal acts laying down rules for algorithmic content moderation, recommendation or decision-making will be to that extent also applicable. Interestingly, also the European parliament Resolution on liability for the operation of Artificial Intelligence-systems expressly refers to AI systems and formulates its own definition[26] for the purposes of introducing a future legal act (Art. 3.a). The resolution establishes a liability regime for the damages caused by AI systems and, therefore, this would be a private-law legal solution compared to the regulatory approach of the AI Act.

[25] The compromise proposed by the Slovenian EU Presidency is available on the Council's public register of documents at: https://data.consilium.europa.eu/doc/document/ST-14278-2021-INIT/en/pdf.

[26] "AI-system" means a system that is either software-based or embedded in hardware devices, and that displays behaviour simulating intelligence by, *inter alia*, collecting and processing data, analysing and interpreting its environment, and by taking action, with some degree of autonomy, to achieve specific goals".

This purpose-specific definition, even if it does not depart from AI Act's definition, does include an express reference to the vital role that data play in the operation, and training of AI systems. Hence, the importance of data-related legal acts is utmost for painting the full regulatory picture for AI.

A more analytical comparison of both definitions invites the following considerations. First, both definitions describe AI systems as software. The resolution on liability makes the distinction between embedded software and standalone software because damages caused by robots and other AI-driven hardware devices are to be clearly addressed. Second, the AI Act is more specific in detailing the techniques that qualify a software as an AI system. To that end, selected techniques are listed in Annex I[27]. The proposal utilizes a more abstract characterization of AI with a reference to 'behaviour simulating intelligence'. Third, both definitions stress the fact that AI systems operates to achieve pre-defined goals. Four, it is interesting to note how the AI Act is more cautious in defining AI systems a software that operates and generates outputs based on human-defined objectives. On the other hand, the Proposal on liability introduces an enticing element of 'autonomy'. Five, both the AI act and the resolution on liability underline the interaction of the AI system with the environment, by collecting and interpreting data and producing actions. The AI Act is simply more specific in defining such actions as content, predictions, recommendations, or decisions. We add in the box below some general extra-legal considerations on the problematic aspects of defining AI based on a review of relevant definitions in the literature (Buiten, 2019).

Box 3: On the problems of define AI for legislative purposes

There is not yet any widely accepted definition of AI even among experts in the field. Various definitions focus on concept of autonomy and intelligence, but there are no objective and future proof ways to characterise what one can consider an autonomous and intelligent computational procedure. The problem for the perspective of law is that what we consider autonomous or intelligent is subjective and will change over time. What we perceived as unpredictable, autonomous, and intelligent outcomes of a computational procedure thirty years ago, it probably appears as nothing special today. If we define AI by intelligence, then the definition is highly contingent on how we as humans perceive outcomes to be intelligent. So, most definitions based on autonomy and intelligence are subjective, circular, and are not future proof. AI becomes what we call AI. But this makes it unsuitable as a basis for laws and regulations. A more pragmatic solution would be what is common to all AI system and applications. The answer is simple: the technology of algorithms. So, policy debates and law making, may be, should focus on regulating algorithms rather than AI systems in general.

[27] (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 optimization method.

In the legal acts grouped under sections 4.1.2. and 4.1.3. there is no definition of AI and, as it is explained below, the term is not even mentioned in the texts. Nonetheless, these legal acts do incidentally define the legal framework for AI in a broad sense either tackling legal issues related to algorithmic systems or laying the foundations of a conducive environment.

4.1.1. Legal acts providing for rules on algorithmic processes and algorithm-driven decision-making

There is a larger number of legal acts whose subject matter is not AI but which they refer to it. They provide for rules on algorithms, algorithmic systems of diverse sorts, automation, or automatic decision-making. In this category of legal acts, the term AI or AI system is not mentioned at all in the legal provisions and only some references to AI, if any, might be occasionally contained in the recitals or the preamble. However, they are relevant in the study if a functional, operational, and/or conceptual link between the definition of AI systems and the variety of algorithmic systems can be explained, as discussed below. The legal acts pertain to this broad category include GDPR, DSA, DMA, or, *inter alia*, P2B Regulation. They refer to algorithmic rating, algorithmic decision-making, algorithmic recommender systems, algorithmic content moderation, algorithmic structures, automated profiling, or a variety of activities and actions conducted by automated means. They include rules related to algorithms, such as: disclosure, risk assessment, accountability and transparency audits, on-site inspections, obtaining consent, etc. As the definition of AI systems proposed by the AI Act reveals, recommendations, decisions, predictions, or content of any kind, as well as resultant actions of the system on or in relation to the environment are natural and frequent outputs of AI systems. Accordingly, legal acts providing rules for algorithmic processes and decision-making in a diversity of scenarios and with a variety of purposes are also relevant to the construction of the regulatory framework for AI in the EU. Provided that the methods and approaches listed in Annex I of the proposed AI Act are used, an AI system may fall under the AI Act as well as under other legal acts to the extent of the specific purpose or the concrete action. As an example, if the system is intended for producing recommendations by a very large platform, DSA (Art. 29) may be applicable; or if the system is applied to profiling, GDPR (Art. 22) may be relevant. In conclusion, understanding the complementarity between the AI-centred legal acts and the range of legal acts that directly or indirectly address the use of algorithms for a variety of purposes and tackle different legal issues arising from algorithmic decision-making is instrumental to depict the full picture on the current and future AI regulatory framework.

4.1.2. Legal acts paving the way for the development of AI

There are other legal acts that, although do not regulate AI and in some cases neither mention it, lay some of the foundations for creating an AI-promoting environment. In this respect, it is worth recalling that the development, testing, training, deployment and use of AI systems do greatly depend upon an environment conducive to promote trustworthiness, fairness, and safety of AI. This category of legal acts concerns cybersecurity, data governance, infrastructure, digital identity, or trust services, *inter alia*. Most of the legal acts falling under this category are not going to be analysed in detail in the study of the interplay and the regulatory gaps, insofar as they aim to settle the general environment for the digital economy without a specific focus on AI.

4.2. Taxonomy of relevant legislative initiatives

In assessing the relevance of the legislative initiatives for the regulation of the AI and before delving into the coherence of the work in progress, the interplay between each initiative and the possible overlaps and gaps, the legislative initiatives must be grouped in three categories based on the proximity to the subject matter: artificial intelligence (AI). While there are legal acts that are intended to regulate, totally or partially, the use, placing on the market or the application for certain purposes of AI systems, others do or may simply impact on the regulation of AI indirectly or incidentally, as the scope of application of the legal act and its policy goals are different and AI is only referred as a tool or an instrument. Listed legal acts, in all categories (existing, proposed, and possible) that are relevant for the EU, can be classified in the following three groups[28].

4.2.1. Legal acts, proposals, or possible initiatives aim to regulate, totally or partially, in a horizontal manner or with a sector-specific approach, the use of AI

The most paradigmatic and clear example would be the AI Act. The AI Act follows a risk-based regulatory approach. AI systems are classified in three groups in the Act preamble and in the related Impact Assessment: unacceptable, high, or low/minimal risk. In the Act itself only 'high risk' and 'other than AI risk' systems are mentioned. Regulatory consequences are prohibition (selected unacceptable-risk uses), compliance of mandatory requirements and ex-ante conformity assessment and post-market monitoring (high-risk uses), and transparency obligations (certain low-risk uses). In complying with the AI Act requirements: providers of AI systems, manufacturers, importers, distributors, users or third parties (if they are deemed providers for the purposes of the AI Act) are subject to a set of obligations. These obligations are without prejudice to other obligations under Union or national law. Therefore, 'the AI Act does not aim to provide an all-embracing, comprehensive regulatory framework for the use, placing on the market or putting into service in the Union'. The scope of application is limited by the specific practices and uses covered (with the subsequent amendments of respective Annexes), the territorial application (Art. 2), and the specific regulatory goal (requirements for the use, placing on the market and putting into service). Other implications or legal issues arising from AI systems, even those covered by the AI Act, do not fall under the sphere of application of the proposal (liability for damages caused, IP rights, consumer protection, etc.). The European Parliament Resolution on liability is aligned with the efforts made in the EU to assess the adequacy of the legacy liability regimes to the distinctive features of AI systems and the effectiveness of the current legal framework (contractual liability, extracontractual liability, defective product liability), both at an EU level and at a national one, to prevent and compensate damages caused by AI. The Expert Group on New Technologies and Liability, divided in two formations (New Technologies formation and Product Liability) tackled these issues and the *Report on Liability for AI and other emerging technologies* was published with a set of findings, recommendations, and guidance. As the Report and the work of both formations reveal, a coherent, effective, and sound liability regime for damages caused by AI system is one of the areas claiming more regulatory attention and a gap to be filled, either by the adoption of new legal acts, as the proposal of the EP, or by the amendment of existing instruments in the Union, namely, the Defective Product Liability Directive[29].

[28] Not surprisingly, these groups widely correspond with the three categories proposed under 4.1 above even if now the perspective is not the definition of AI but the impact of the legal act on the subject matter.

[29] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products. Directive 1999/34/EC extended the scope of liability to agricultural and fishery products.

4.2.2. Legal acts, proposals, or possible initiatives whose subject matter is not explicitly the AI, but they deal with aspects, features, properties, or dimensions of AI and its impact on the economy.

AI systems are designed, developed, put in service, distributed, operated, and used in a technological and regulatory environment. Thus, the regulation of converging technologies and the digital environment does impact on the reliability, the quality, the safety, or the efficacy of AI. AI and other emerging digital technologies share some disruptive features that explain the need to revisit current concepts and reconsider existing rules. These distinctive characteristics, of disruptive potential, are[30]: autonomy, complexity, opacity, openness, data dependence, and vulnerability. Accordingly, those legal acts aimed to either counter the negative effects of these distinctive features – i.e., laws on cybersecurity to mitigate the vulnerability -, or to provide a legal framework conducive to foster the positive effects of such features – i.e., data-related acts facilitating the free flow of data for AI-related purposes. The feature-based description of AI as proposed above provides helpful guidance in assessing the interplay of relevant legal acts.

a) Data use and reuse, data sharing, database protection

AI's training, development, and effective operation is highly dependent on the availability, reliability, accuracy, and sufficiency of data. Therefore, legislative initiatives promoted by the European strategy for data and pertaining to the data economy affect AI as far as data dependency is concerned. Data-related legal acts' relevance for AI is two-fold: data availability, accessibility, and use/re-use, on the one hand; and protection tools for investment in collection, processing, and aggregation of data.

AI development benefits from all efforts to foster data-driven innovation and economy. The EU has put in place a solid and entrenched legal framework for the protection of personal data with the GDPR and the ePrivacy Directive. Concurrently, the Open Data Directive in combination with the Data Governance Act would pave the path to facilitate data sharing with an important role of data sharing intermediaries under the FAIR data principles. In addition, the Data Act would complement a legal framework conducive to a fair allocation of data value among actors of the data economy, especially B2B (data sharing, portability, safeguards of non-personal data in international contexts). AI and technologies enabling data analytics and fed by machine-generated data are commonly dealing with mixed datasets consisting of both personal and non-personal data. Therefore, a consistent approach interlinking personal data protection rules and non-personal data legal framework is critical to foster AI in the Union. The GDPR and the Regulation on the free flow of non-personal data provide for the free movement of 'all' data within the EU. The Regulation on free flow of non-personal data lays down a general prohibition against data localisation requirement (Art. 4.1) unless justified on grounds of public security; whereas the GDPR provides for the free movement of personal data within the Union without restrictions on the grounds of protection of personal data. Thus, the complementarity between the GDPR and the Regulation on free flow of non-personal data, on free movement of data within the Union and data portability, does also reinforce the development, the training, and the operation of AI systems

[30] Commission Staff Working Document, Liability for emerging digital technologies - Accompanying the document Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, Artificial intelligence for Europe, SWD(2018) 137 final. Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee, Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, COM(2020) 64 final, Brussels, 19.2.2020. Report on Liability for Artificial Intelligence and other emerging technologies, available at: https://op.europa.eu/en/publication-detail/-/publication/1c5e30be-1197-11ea-8c1f-01aa75ed71a1/language-en-.

in the EU. Hence, the legal acts implementing the EU strategy on data economy do not directly address AI as the AI Act and the Proposal on Liability, but they impact on the fuel that the AI needs to learn and develop. In that regard, the interplay crystallizes in a relation of complementarity. Policy goals and scopes are different but converge in the resultant effect: an environment favourable to the development of safe, reliable, and trustworthy AI.

Investment in sophisticated systems for collecting, processing, and organizing data is vital to the data economy. The concepts, rules and principles underpinning the Database Directive upon its adoption need to be reconciled today with the technological advances and the policy goals pursued by the EU to foster a thriving data economy and data-driven innovation. Latest developments in data processing, big data analytics, and database production are very closely linked to the burgeoning of AI and challenge the Database Directive logic. In the absence of a proper adaptation of the Database directive to the new scenario where AI plays the leading role, a regulatory gap may materialize. AI development and operation might be disincentivised if the Database Directive happens to have a deterring effect on AI investment. But, concurrently, an expansion of the *sui generis* protection enshrined by the Database Directive might interfere with the policy goals of the EU Data Economy strategy in relation to the access to data. The distinction between purely collecting and systematizing tasks (traditional database making) and data creation activities (updating, maintenance, publication, curation). The impact of expanding the database protection to data creation on data access for the development of AI. This interplay, as described above, is conflictive. The Database Directive in its current version contradicts or may counter the efforts to unleash the potential of AI for Europe. Thus, more than a regulatory gap, a potential conflict of policies is to be untied.

b) Cybersecurity and resilience

Vulnerability is another distinctive feature of AI systems. Cybersecurity plays a crucial role in ensuring that AI systems are resilient against attempts to alter their use, behaviour, performance or compromise their security properties by malicious third parties exploiting the system's vulnerabilities. Cyberattacks against AI systems can cause damages with massive losses or alter the functioning of critical infrastructures managed and operated by AI systems. The AI Act acknowledges the criticality of certain AI systems that classify as high-risk (Annex III) and the need to minimize the vulnerability of these systems by ensuring a level of cybersecurity appropriate to the risks. Thus, suitable measures should therefore be taken to provide accuracy, robustness and cybersecurity in the design and the development of high-risk AI systems. (Art. 13, Art. 15). The interplay between the AI Act requirements on cybersecurity and the Cybersecurity Act (Art. 42.2 AI Act) is the presumption that high-risk AI systems that have been certified or for which a statement of conformity has been issued under a cybersecurity scheme pursuant to the latter Regulation 2019/881 shall be presumed to follow the cybersecurity requirements set out in Article 15 AI Act. Besides, the AI Act expressly recognizes the application of the Regulation 2019/1020 on market surveillance and compliance of products to AI systems covered by the AI Act with the needed adaptations: extensive concept of economic operator to include all operators of the Title III, Chapter 3, AI Act, and definition of product as to cover all AI systems falling under the scope of the AI Act. The interplay with existing sectoral safety legislation is ensured by integrating in the conformity assessment procedures the checks of the AI requirements (new legislative framework) and by considering the requirements of the AI Act in the adoption of relevant implementing or delegated legislation under the old approach legislation. (i.e., Art. 82 in relation to Regulation 2019/2144 on motor vehicles or the incorporation of the conformity assessment and the provider's procedural obligation into the Directive 2013/36 for credit institutions). It must be noted that, the earlier cited compromise text of the Slovenian Presidency introduced proposed

changes relevant to this matter. First, apparently EU Member States have obtained that security competence are exclusively nationals and that AI systems developed exclusively for military purposes should be taken out of the scope of the regulation. Second, the possibility of using biometric identification systems in real-time has been extended to actors that are not law enforcement authorities but are collaborating with them. Third, the reason for employing these systems has been extended to protect critical infrastructure.

c) Opacity versus transparency

Transparency has been a constant in several legal initiatives aimed to ensure fairness, well-informed decisions, reduction of information asymmetry or protection and enforcement of rights. Transparency is also deemed as an effective policy tool to counter the opacity of AI systems that would make their operation incomprehensible to or too complex for natural persons. Opacity may describe two situations. First, the fact that the process, the decision, or the interaction is performed by automated means. Disclosing the fact that the system is automatic (decision-making, facial recognition, content generation, profiling, etc.) would allow persons to adopt informed decisions, minimize the manipulative or misleading effects, and enable objection to be subject to such automated processes. The AI Act relies on transparency with such purpose for systems that interact with humans, detect emotions, or generate or manipulate content ('deep fakes'). Likewise, disclosure of the automated nature of the decision is also presumed in Art. 22 GDPR as a prerequisite to exercise the right to object. Second, the parameters, the conditions, and the criteria an algorithm-driven system works on. From this perspective, transparency and explainability are policy solutions commonly shared by DSA, P2B Regulation or DMA. Transparency obligations in the AI Act for high-risk systems goes further and refer to clear instructions for use and other relevant information for the users (Art. 13).

d) Autonomy and complexity

Complexity and increasing autonomy are features that clearly impact on the application of traditional liability rules to damages caused by AI systems. The inherent complexity of AI systems renders the identification and the proof of the possible causes and the liable person/s particularly difficult, costly, or onerous for the victim. Besides, the learning capabilities of the AI system may lead to increasingly autonomous decisions whose consequences depart to a certain extent from the expected pre-determined performance. In such cases, the causal link debilitates, and the allocation of risk and liability becomes a challenging task. Therefore, all efforts to adapt liability rules to face the challenges posed by complex, autonomous AI system will contribute to the consolidation of the AI legal framework and the filling of the gaps opened by these characteristics of AI systems: complexity and autonomy. The definition of AI system formulated by the Proposal on liability as described above underlines the element of autonomy and tackles the problems that assuming a level of autonomy may entail. First, in the definition (Art. 3.a) a certain degree of autonomy in taking actions and adopting decisions to achieve the goals is accepted. That debilitates the link to attribute the damaging consequences. However, to prevent a situation of undercompensating or non-compensating victims at all on the sole basis of the technology user, the Proposal on liability warns that autonomy is not per se a defence for the operator under the fault-based regime. Article 8.2 in fine is clear when declaring that '(t)he operator shall not be able to escape liability by arguing that the harm or damage was caused by an autonomous activity, device or process driven by his or her AI-system'.

4.2.3. Legal acts that provide for rules related to algorithmic decision-making

Relevant legal acts contain several provisions on algorithmic decision-making, processes, or tasks (GDPR, DSA, P2B Regulation, *inter alia*). Some provisions provide for specific rules related to the use of algorithmic decision-making – such as Article 22 GDPR on profiling or Article 29 DSA on algorithmic recommender systems – while others are drafted as enabling provisions for the use of automated means – content moderation or complaint-handling by automated means in DSA Articles 14, 15 o 17. Algorithm-centred provisions complement the legal framework for AI insofar as they address certain uses, applications, or purposes. In the analysis of the regulatory gaps below, these provisions will be considered.

The focus of these legal acts is not the AI, but they provide for rules that do incidentally impact on the legal regulation of AI insofar as they deal with obligations linked to the implementation of algorithmic-driven mechanisms. From these rules, certain principles can be inferred to trace the regulatory contours of AI.

5. REGULATORY GAPS AND COHERENCE

The analysis of the interplay between the selected legal acts, directly or indirectly regulating the development, placing on the market, putting into service or use of AI systems, or other AI-related aspects, or issues arising from algorithmic processes and decision-making may reveal intended or inadvertent regulatory gaps. We classify regulatory gaps in three categories: a) regulatory gaps *strictu sensu* (see below); b) l*atu sensu* interplay gaps (where interplay creates a space that remains uncovered or where it creates uncertainty for market players); c) implementation postponed gaps areas where the legislative act postpones (possibly problematic issues are not addressed in the legal act and will become part of the implementation phase). Since type (c) has been widely discussed in the previous three chapters, in this one we focus on gap *strictu sensu* and on areas of lack of coherence in the interplay between legislative acts. Most prominent example of type (a) are:

- A narrow delimitation of the scope of application or a questionable exclusion from the scope of a relevant act;
- An absence of substantive rules governing a specific issue deserving regulatory attention;
- An unintended unregulated space due to the drafting/wording of legal provisions; and
- A space uncovered by interrelated legal acts.

We do this with a specific focus on AI (section 5.1) and on its interaction with data protection and privacy (section 5.2), and with cybersecurity (section 5.3). Other noteworthy gaps are briefly reviewed in section 5.4. Finally, in section 5.5 we present a summary taxonomy of gaps. As anticipated in the introduction, AI is currently the cornerstone of digital legislation, and relatively more space is dedicated to it in section 5.1 where, however, besides the AI act its interplays with other legislative acts are amply discussed.

5.1. Focus on AI Act and interplay with other legislative acts

5.1.1. The scope of application of the AI Act

Regulatory gaps will be first identified within the AI Act. By delimiting the scope of application, the AI Act delineates the contours of the regulatory perimeter, excluding or not addressing certain purposes, uses or sectors. In that regard, it might be argued that the AI Act leaves certain gaps uncovered. While in some cases uncovered regulatory gaps are unintended and require a discussion about how they should be addressed, in other cases identified gaps may represent a policy decision. Finally, in other cases, they are the results of a misinterpretation and thus require a clarification.

The gaps identified in the original proposal are listed below and integrated with considerations on the changes introduced by the Joint Compromise of 29 November 2021.

The following gaps in the AI Act are identified:

1. **AI Act, Article 5**: the list of prohibited AI practices and uses in Article 5 doesn't cover a few AI practices, which are instead addressed by the Joint Compromise. In particular:
    a. **Social scoring leading to detrimental/unfavourable treatment.** It was argued[31] that social scoring by private entities non acting on behalf of public authorities should be

[31] EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18 June 2021. The reason behind the opinion of the EDPB-EDPS was basically logical

prohibited together with any social scoring practice implemented by social media and cloud service providers. The Joint Compromise, amending Article 5(1)c of the AI Act by erasing reference to 'public authorities or on their behalf', seemingly goes in the direction of closing this gap, insofar as it extends the prohibition of social scoring beyond its initial use by public authorities;

b. **Biometric identification systems**. It was argued[32] that the definition of biometric AI systems in the proposal creates some inconsistency, which lends support to calls for banning their uses in non-public spaces for purposes other than law enforcement, or not in real-time. The amendments to Article 5(1)(d) agreed by the Joint Compromise do not fully incorporate the proposed expansion of scope. The scope of the prohibition for real-time use of biometric systems has been reduced. The amendment of Article 5(1)(d) clarified that real-time remote biometric identification systems in publicly accessible spaces could also be used by other actors, acting on behalf of law enforcement authorities. Moreover, the list of objectives for which law enforcement should be allowed to use real-time remote biometric identification, included also in Article 5(1)(d), has been slightly extended;

c. **Military purpose AI systems**. The general exclusion from the scope of the AI Act of AI systems exclusively developed or used for military purposes has been questioned upon the adoption of the Proposal. The Joint Compromise proposes the adding of a justification of such exclusion in Recital 12 AI Act. As national security remains the sole responsibility of Member States (Article 4(2) TEU), AI systems that are used or developed with an exclusive national-security purposes remain excluded from the AI Act. The Joint Compromise would be then confirming that an unnoticed regulatory gap is absent in the AI Act in relation to AI systems for military purposes, but the exclusion responds to a political decision. Nonetheless, the added clarification in Recital 12 as per the amendments proposed by the Joint Compromise reaffirms that the exclusion is purely purpose-based. Therefore, dual-use AI systems would fall under the scope of the AI Act; and

d. **AI system for research**. The application of the AI Act to systems specifically developed and put into service only for the purpose of scientific research and development activity is unclear. The risk of an undesired deterring effect on freedom of science and of an undermining impact on the development of research activity has been noted. The Joint Compromise proposes the adding of a new Recital 21a to clarify to which extent AI Act applies to AI systems specifically developed and put into service only for scientific research: not applicable, if the purpose is only to conduct basic research;

and by analogy. The opinion notes that, in view of large discrimination risk, the AI Act proposal prohibits social scoring, if performed over a certain period of time or if performed public authorities or on their behalf. Then, it derives consequentially that the ban should include private companies (the opinion cites social media and cloud service providers), since the process vast amount personal data and conduct social scoring over long time periods. So, for the sake of symmetry, the opinion argues, the AI Act should prohibit any type of social scoring.

[32] The EDPB-EDPS joint opinion also noted that the first version of the proposal has some conceptual shortcoming on biometric AI systems, resulting in an incoherent account of their collective risks .See for instance the analysis provided in L. Belkadi 'The Proposed Artificial Intelligence Act and Biometric Systems: A Peek Into the Conceptual Maze', Law KU Leuven blog, 3 November, 2021 (https://www.law.kuleuven.be/citip/blog/the-proposed-artificial-intelligence-act-and-biometric-systems-part-ii/).

applicable, if the purpose is the conduct of any research and development activity that may lead to market deployment.

2. **The purpose-specific approach**. The AI Act is based on a purpose-specific approach. Thus, the classification of AI systems on a risk basis relies on the use or purpose. Such a scoping strategy raises the question of general-purpose and multi-purpose AI systems. It is doubtful whether general-purpose AI system[33] would be subject to the proposal and, if so, to which extent, insofar as the risk-based classification and the relevant obligations require a prior determination of the purpose. The proposed Article 52a by the Joint Compromise intends to close the regulatory gap by clarifying the application of the AI Act and the identification as a provider of the AI system to any person placing on the market or putting into service a general-purpose AI system 'for an intended purpose that makes it subject to the provisions' of the proposed Regulation. The Joint Compromise also proposes to exclude from the scope of the AI Act application a new category of general-purpose AI systems unless they are put under a trademark or integrated into another system subject to the regulation;

3. **AI Act, Article 6**: it is argued that AI systems (scoring, rating) used in the insurance sector seem not to be covered neither by Annex II nor by Annex III[34]. The proposed amendment of the Joint Compromise to Annex III, point 5, would fill that regulatory gap insofar as it explicitly includes high-risk AI systems 'intended to be used for insurance premium settings, underwritings and claims assessments';

4. **AI Act, Article 7**: Annex III can be properly updated by the Commission. The above-mentioned gap may be filled either by redrafting the text before approval, or by a future amendment of the Annex III, or by providing guidance in interpretation, or by confirming the intended exclusion from the scope of application. The proposed drafting of the Joint Compromise of Article 84 may decrease the adaptability of the AI Act to future technological advances and AI uses (future proof), as paragraph 1.b delays the assessment of the Commission of the need for amendment of the list in Annex III to a 24-month period. Even if such an extension reduces the burden on the Commission to pilot and monitor the review of the AI Act and the costs of regular revision, it might fossilize the AI Act scope in the facing of the exponential growth of technological applications. Nevertheless, Art 7 AI Act is always enabling the Commission to adopt delegated acts where needed. The combination of Art 7 and the new Article 84 as proposed by the Joint Compromise may succeed in striking a balance between the aspiration to embrace new AI uses and the minimization of the cost of review;

5. **AI Act, Article 4.** The same reasoning applies to the definition of AI system as per the AI Act and the agility of the procedure to amend the techniques listed in Annex I, pursuant to Article 4. These considerations reveal a potential regulatory gap if the definition of AI or the listed techniques and approaches under Annex I (unintendedly) leave outside the scope of the AI Act practices, solutions or systems that should be covered by the legal act in conformity with its policy goals.

   By establishing an amendment procedure for the Commission to update the list of Annex I by the adoption of delegated acts, the legislator is assuming that the scope of the proposed legal act (AI Act) can evolve. In determining the definition of AI systems, for the purposes of the

[33] It should be noted that, according the GDPR, general-purpose AI systems would not be allowed to collect personal data.

[34] Annex II contains the list of Union harmonisation legislation, while Annex III contains the list of High-Risk AI systems referred to in Article 6(2).

proposed legal act, on the basis of the techniques and approaches listed in Annex I, there is a policy decision to include certain techniques and exclude others at the time where the AI Act is adopted. In that regard, if the initial list is very limited it might be always argued that there is potentially a regulatory gap: those techniques and approaches that are not, at least in the initial list, covered by the AI Act. For example, if there are techniques other than those listed in Annex I but functionally equivalent to them that can be used in AI system – as Art. 4 does precisely set out 'characteristics that are similar to the techniques and approaches listed' in Annex I. But as in many other aspects of the proposed legal acts, there is not a pure regulatory gap if the delimitation of the scope and, therefore, the exclusion of certain techniques and/or of specific AI systems from the AI Act is not unintended but a conscious policy choice. The evolution of the definition of AI systems in the AI Act exemplifies how the policy compromise has to crystallize in the final drafting of the legal provision. During the negotiations, it has been discussed whether the scope of the AI Act should cover any automated system or solely those systems that can be classified as 'learning systems'. Accordingly, the list of techniques and approaches in Annex I should be adjusted to a wider view or to a narrower view instead. Should the narrower view prevail, it can always be asked which legal regime, if any, applies to the systems not falling under the scope of the AI Act.

Art. 4 AI Act will indeed work as a gap-filling mechanisms provided for by the same legal act to keep the legal framework up to date to market and technological developments;

6. **Low risk AI systems and Article 67 AI Act** – It cannot be totally excluded the possibility that a low-risk AI system, despite not having been classified as a high-risk AI system, may present a risk to the health or safety for persons as referred by Article 67 AI Act. However, it seems that Article 67 AI Act cannot apply to compliant low-risk AI systems. That means that the only way to mitigate the risk and ensure the appropriate measures is to amend the Annex III and include the concerned purpose or use. It might be reconsidered this methodology and provides for more granular application of certain duties or provisions.

   In particular, the resort to codes of conducts to incentive voluntary compliance of requirements by AI systems other than high-risk AI system may contribute to such a granular application (Art. 69 AI Act); and

7. **Mixed high-risk/low-risk AI systems**. Insofar as the classification of AI systems as high-risk in Annex III is based on purpose or use, it is plausible and likely that providers put on the market AI systems of a mixed nature due to the combination or the convergence of listed high-risk purposes and non-listed purposes. If that happens, the providers need to know whether the two regulatory regimes should be applied: high-risk AI system requirements to the part of the system performing such high-risk purpose, and low-risk AI system requirements to the rest, if that is feasible, or, on the contrary, the high risk absorbs the low risk and then it prevails. Then, as soon as a high-risk purpose, even incidental or minor, is pursued by the AI system the strictest high-risk regime applies. The AI Act does not provide for an express rule or guidance for the providers to assess compliance in such cases of mixed AI system. This case may recall the solution provided for mixed databases where personal and non-personal data are closely linked. Clarification in the proposed legal act (AI Act) how to manage complex and mixed AI system may desirably increase legal uncertainty.

5.1.2. Interplay between AI Act and other legal acts

The interplay between the AI Act as the core component of the AI regulatory framework and other legal acts, as identified below (rules on sandboxes, liability rules, defective product liability and strict liability regimes) reveal some doubtful areas:

1. **Title V. Art. 53 AI Act - AI Regulatory sandboxes**. Subject to further implementing acts, a proper coordination between AI regulatory sandboxes and other ongoing or future sandboxes (financial sandboxes, mobility sandboxes) within the EU needs to be guaranteed, as many innovative projects eligible in other sandboxes do frequently incorporate AI solutions. As an illustration, the financial sandbox implemented in Spain by Law 7/2020, of 13 November, *para la transformación digital del sistema financiero*. (Official Bulletin BOE 14 November 2020), Title II, Articles 5 and following. A need of coordination with existing laws, but more importantly with future initiatives in other EU states, is to be alleged;

2. **Burden of proof for non-compliance of obligations.** The effects of non-compliance of obligations and requirements, laid down in the AI Act, by the relevant actor on the application of extracontractual and defective product liability rules remain unclear. The compliance or non-compliance of certain obligations laid down by the AI Act may trigger (rebuttable) presumptions for the purposes of attributing liability and allocating the burden of proof. The allocation of burden of proof is mainly regulated by national law as EU tort law is not harmonized. In that regard, domestic liability rules or procedural rules establish the level of proof and the allocation of the burden of proof in general. At the EU level, there is a harmonized regime though for defective products[35]. Under this regimen, the injured person shall be required to prove the damage, the defect and the causal relationship between defect and damage. According to a recent report of the Expert Group on Liability and New Technology set up by the Commission (European Commission, 2019), logging requirements should protect the victims. AI systems should have logging features to monitor activities, in absence of which or in case of failure to provide logged data, the burden of proof should be reversed;

3. **High-risk category (Art. 6 AI Act) and liability rules**. Additionally, it is not clear whether the high-risk category under the AI Act is consistent with the liability rules for damages caused by AI systems. Specifically, to which extent the designation as a high-risk is consistent throughout all relevant regulations and whether the high-risk category should lead to the application of strict liability[36] regimes in any event. Traditionally, the high risk posed by an activity (keepers of animals, motor vehicles, immovables in unsafe conditions, etc.) is an argument for applying strict liability to the 'keeper of a source of danger'. Consequently, a strict liability system would efficiently allocate the incentives to adopt the duty of care and adapt the level of the high-risk activity. Non-contractual liability rules, either being fault-based or risk-based regimes, are essentially at a national level. At an EU harmonized level, the product liability regime is arguably a case of strict liability (even if there is scholars' debate on whether there is a genuine strict liability regime or, on the contrary, the product defect is indeed replacing the concept of diligence as inspiring a fault-based liability regime). The aim of the Directive on defective product liability (Directive 85/374/EEC and Directive 1999/34/EC) is precisely to hold the manufacturer strictly liability for damages caused by defect in the products put on the market.

[35] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products.

[36] Strict liability means liability for injury or damage to another person without fault.

The emergence of AI system has revitalized the rationale behind the strict liability. Thus, if AI is deemed to be a source of danger that is likely to increase the ordinary risk of any activity, a case for a strict liability regime for damages caused by AI system is put forward. That is the interlink between the definition of high-risk in the AI Act and the relevance for the purposes of liability. In fact, a connection can be found between the notion of high-risk under the AI Act and the risk-liability regime proposed by the Proposal on Liability. According to this proposal, fault-based liability is the liability regime by default. Strict liability rules are provided for certain AI systems designated as high-risk, which is defined as 'a significant potential in an autonomously operating AI-system to cause harm or damage to one or more persons in a manner that is random and goes beyond what can reasonably be expected; the significance of the potential depends on the interplay between the severity of possible harm or damage, the degree of autonomy of decision-making, the likelihood that the risk materializes and the manner and the context in which the AI-system is being used' (Art 3. Proposal on liability). Even if the description of high risk might be aligned with the high-risk category under the AI Act, the Proposal on liability adopts a list-based approach, which is different. Article 4.2 refers to an exhaustive, amendable by delegated act list enumerating which high-risk AI systems are subjected to strict liability. Still the opened question is whether an alignment or any kind of mutual interaction between the definition of high-risk in the AI risk and the application of strict liability is needed or there are distinct and separate legal systems with different policy goals to meet; and

4. **Causal link (Article 62 AI Act) –** liability rules. By regulating reporting duties of serious incidents and malfunction of high-risk AI system, Article 62 AI Act states that the providers of such systems have to notify any serious incident or any malfunctioning that entail a breach of obligations under Union law to protect fundamental right 'immediately after the provider has established a causal link between the AI system and the incident or the reasonable likelihood of such a link'. The drafting of this provision brings about an interesting and uncertain interplay of AI Act and liability rules. Is Article 62 AI Act a provision aiming to allocate a burden of proof for the purposes of placing liability? Shall the causal link established by the provider for the mere purposes of reporting incidents be relevant for attributing liability? Can that determination of the causal link be deemed an assumption of liability by the providers? And finally, on which grounds should that causal link by reasonably established by the providers?

In that regard, the coordination with a future/possible legal action on liability for AI systems will be fundamental.

5.1.3. Liability for damages caused by AI systems

The adequacy of the liability rules to properly address and compensate damages and losses caused by AI system is a critical issue in the shaping of a flawless regulatory framework for AI in the EU. We should distinguish here between (i) strict and fault-based liability and (ii) defective product liability.

Strict and fault-based liability. In the absence of an AI-centred proposal as the one proposed by the European Parliament resolution of 20 October 2020, the application of existing liability rules to damages caused by AI system is challenging. As the Expert Group *Report on Liability for AI and other emerging* technologies underlined, there are challenges in the application of legal liability systems that deserve attention. *Inter alia*, the identification of the liable person might be difficult considering the complexity of technological ecosystem with multitude of providers, components, and services. The opacity and the vulnerability invite reconsidering the traditional placing of the burden of proof. The increasing autonomy, the openness, and the data-dependency of AI systems may require further monitoring of the system after the market placement.

Thus, if a European initiative for the liability of AI systems is not adopted, the liability rules may not be suited to accommodate the challenges of AI leading to uncompensated or undercompensated victims. Besides, the liability regime would remain unharmonized within the Union. Not only inharmonious among the Member States, but also potentially disparate compared to the protection (level of compensation) provided to victims of damages caused by other technologies.

Defective product liability. Being the defective product liability regime harmonized at the EU level, its consistency with the efforts to provide comprehensive rules for AI systems is particularly critical. A public consultation[37] collected information, findings, and views on the need to adapt the Product Liability Directive for addressing products in the digital economy and the circular economy. Concerns are related to the concept of product (AI as service or complex product of interconnected devices with multiple, changing components), the proof of defect and causal link, the identification of the producer (or liable person), the extent and scope of the defences (later-defect defence, development risk) and the impact of upgrading and updating the product after the market placement.

5.1.4. Liability exemptions for intermediaries and use of AI systems under the DSA

The interplay between the liability exemption – under e-Commerce Directive as revisited in the DSA – and the intensive use of algorithmic decision-making in content moderation, notice and removal, complaint-handling or conflict solving is a critical issue. The DSA does not ignore the interplay, but it requires further discussion. There are friction points in several aspects:

1. **Article 7 in relation to Article 6 DSA**: Whether the deployment of a large-scale algorithm content moderation system may entail de facto general monitoring;
2. **Article 4.1.e) and Article 5.1.b) DSA**: Whether the poor performance of algorithmic voluntary measures failing to detect (illegal/inappropriate) content should be interpreted as explicit operators' knowledge and trigger the duty to react and the resultant liability;
3. **Article 22 DSA**: How to determine under Article 22 DSA the liability of the platform operator vis-à-vis the party who is relying on the trader's information if the data are inaccurate, outdated, unverified, unverifiable, false. Is the platform a Trusted Third Party?;
4. **Article 22 DSA in relation to Article 5.3. DSA**: How to apply Article 22 in the relation with Article 5(3): if the information relating the transactions is presented in a way that it leads consumers to believe that information was provided by platforms or under their authority or control, besides excluding exemption of liability, might it render the platform liable for the information of the trader as well? Would the platform become the 'contracting party' (trader)?; and
5. **Article 5(3) DSA and the consequences on contractual liability**: In a close connection with the previous issues, might the consumer enforce contractual remedies against the platform? It is unclear whether Article 5(3) DSA goes beyond the liability for the platform for the information of the trader and might entail that the platform operator is placed at the position of the trader as contracting party vis-à-vis the consumer. The wording of Article 5(3) DSA seems to be limited to liability for the trader's information, but a deeper reflection is advisable. The consumers' expectations as regards to the actual contracting party might trigger further liability

[37] Civil liability – adapting liability rules to the digital age and artificial intelligence, Public consultation, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Civil-liability-adapting-liability-rules-to-the-digital-age-and-artificial-intelligence/public-consultation_en. The public consultation period ended on 10 January 2022.

consequences. An eventual integration of the contract with the trader's information may lead to contractual liability. That invites a careful consideration of the remedies available for consumers in the EU consumer protection framework.

5.1.5. Attribution of legal effects

In the context of contracts concluded by electronic means, while the e-Commerce Directive recognises the validity and enforceability of such contracts, it remains unclear whether self-executed contracts (smart contracts meeting the requirements to be qualified as legal contracts) shall not be denied legal effects solely on the grounds that are coded in machine language and self-executable. This might fill a gap that has not yet been addressed in the EU. Divergent national legislation on this issue would fragment the internal market in the development of AI/algorithms applications. There is still uncertainty on this point because, despite the relevance for these purposes of Article 12 of the United Nations on the Use of Electronic Communications in International Contracts:

- No EU Member State has ratified the Convention;
- Article 12 does not necessarily cover either the conclusion of contracts in machine language or the performance of self-executing obligations resulting from a smart contract; and
- Article 12. Use of automated message systems for contract formation. A contract formed by the interaction of an automated message system and a natural person, or by the interaction of automated message systems, shall not be denied validity or enforceability on the sole ground that no natural person reviewed or intervened in each of the individual actions carried out by the automated message systems or the resulting contract.

Clarifying the stance of the EU on the validity of smart contracts would also facilitate the decisions on the attribution of legal effects arising from the use of AI systems beyond civil liability: whom to attribute contractual rights and obligations, decisions, or actions with legal relevance adopted or performed entirely by AI/algorithm-driven systems.

5.1.6. Algorithmic transparency

A thorough analysis of the regulatory gaps in relation to algorithmic transparency should jointly consider Article 22 GDPR, the transparency requirements laid down in the AI Act, the provision on ranking of the P2B Regulation or the provisions on recommender systems for very large platforms in the DSA. The joint analysis of these legal acts that we carried out confirms that the transparency, disclosure, and explanation of parameters, criteria, or conditions under which certain algorithm-driven systems work is a fundamental horizontal policy decision that should be taken at the EU level and where existing and proposed acts show little coherence. Comparing the scope of application of the relevant provisions as set out in the above-referred legal acts (GDPR, DSA, P2B Regulation) does show an incomplete picture with some regulatory gaps needing attention. The scope of application of the P2B Regulation is limited to online intermediation services (Art.2.2) that only cover transactional (or pre-transactional) platforms for B2C relationships. Then, its provisions do not have impact beyond then. While the DSA's scope is significantly wider, the duties related to recommender systems are imposed to very large platforms. Thus, transparency requirements provided for by the P2B Regulation (Art. 5) do only apply to providers of online intermediation, while transparency requirements laid down in DSA (Art. 29) are only applicable to very large platforms. Providers other than providers of online intermediation services covered by the P2B Regulation and platforms that are not very large platforms are not subject to such transparency requirements as respectively provided by the two legal acts.

But additionally, the transparency requirements of the P2B Regulation are only applicable to ranking, whereas the ones laid down in the DSA are exclusively related to recommender systems. Other algorithmic systems are not regulated by the referred legal provisions (Art. 5 P2B Regulation and Art. 29 DSA).

Yet, GDPR focuses on decisions 'based solely on automated processing' (Recital 71 and Art. 22) and it is not clear the extent and the meaning of a purported right to explanation. Hence, Art 22 GDPR requirements applies neither to partially automated processes that combines human and automated processing nor vis-à-vis a person other than the data subject affected by the decisions adopted by profiling, even if it is based solely on automated processing. Article 23 DSA applies to platforms – and very large platforms by accumulation in the staggered model implemented by the DSA – and adds to the general transparency reporting obligations laid down in Article 13 other items. But the obligation imposed in Article 23 DSA is just limited to the 'use of automatic means' not the criteria and the algorithmic patterns, and solely those automatic means used for the purpose of content moderation.

The above-noted illustrations reveal that there are regulatory gaps in the transparency requirements in relation to the personal scope of application (who has the duty to disclose or inform) as well as the objective scope of application - which algorithmic system is covered (ranking, recommender system, content moderation, etc.).

Among these items, it must be mentioned the one included in paragraph 1 letter c) as it is aligned with the policy of advising the user on certain decisions adopted by automated means. In fact, online and very large platforms must include in the report 'any use made of automatic means for the purpose of content moderation, including a specification of the precise purposes, indicators of the accuracy of the automated means in fulfilling those purposes and any safeguards applied'. There is no other limitation or consequence deriving from the use of automated means for such purpose other than the need to report it. Along the same lines, all these legal acts contain references to 'human review', 'human oversight' or 'human intervention'. It would be advisable to clarify the policy on this matter. Whether there is a right to ask for human intervention and then when and on which conditions. Whether human oversight is a duty, when and to which extent. Whether human oversight is a measure to be adopted on AI systems in any event and which consequences may arise from non-compliance. Thus, in this case, the gap refers to a lack of totally homogeneous and consistent policy approach and regulatory treatment that may require further consideration.

In concluding on AI and the AI Act it is worth adding the extra-legal considerations included in next text box.

Box 4: The debate on error-free datasets for AI systems

The expectation that 'Training, validation and testing data sets should be sufficiently relevant, representative and free of errors and complete in view of the intended purpose of the system" (Recital 44) is unrealistic. Most public datasets are incomplete and, it is suggested, it would be better to talk of thresholds (Floridi, 2021, p. 219). According to commentaries (see for instance Bertuzzi, 2021) on the debate among Member States at the time the Joint Compromise text was leaked to the press, it seems that also several EU countries stressed that requiring data sets that are complete and free of error might be unfeasible. Such commentaries also noted that the excessive administrative burden for SMEs was a recurrent theme in the discussions, an issue that was also raised at the last summit of EU heads of states. The requirement of complete datasets may turn into a gap because of inapplicability during the implementation process. Whereas the issue of administrative burden might become the basis for opposition and other changes as the legislative process of the Act continues.

5.2. AI, data protection, and privacy

The interplay between the AI Act and the GDPR is multi-fold and conspicuous. The AI Act acknowledges that its provisions are without prejudice of any other EU legal acts the operators of AI systems must abide by, in particular, data protection regime (Recital 41 AI Act). And more explicitly, the AI Act (Recital 41) stresses that it should not be interpreted as providing the legal ground for processing of personal data. But such a generic statement of compatibility between the AI Act and the personal data protection regime may not be sufficient to cover all possible use of data by AI systems. Therefore, more clarity in the AI Act as regards the processing of personal data is needed and, consequently, some regulatory gaps can be singled out.

a) Scope of AI Act, prohibited practices under Article 5 from the perspective of compatibility with fundamental rights

Soon after the adoption of the AI Act, some claimed that the act does not protect individuals from harms sufficiently, for it does not engage with the limitations in international human rights treaties and the EU Charter regarding the protection of fundamental rights in the digital context (Krupi, 2021). In the analysis of the prohibited AI practices and uses listed in Article 5, some of the practices have been mentioned as uncovered in paragraph 5.1.1 above, with additional changes in opposite directions introduced by the Slovenian Presidency compromise text of 29 November 2021. Additionally, from the perspective of the compatibility with 'fundamental rights' and with personal data protection, other practices are arguably[38] missing in the scope or under-classified – allegedly, they should be prohibited or reclassified as high-risk. The following practices might be taken into consideration in the assessing of possible regulatory gaps. As previously noted, the drafting decision to include or exclude and the final classification of specific practices, as listed below, depend upon a policy decision, and therefore, they do not constitute a regulatory gap if it is based on a policy option.

(i) Any social scoring performed by social media and cloud service providers might be deemed as a prohibited practice – as the proposal of the Joint Compromise, as detailed above, suggests.

(ii) Biometric identification systems used in public spaces should include not only facial recognition, but also gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals.

(iii) Emotion recognition systems powered by AI may have highly undesired discriminatory and dignity consequences, manipulative effects, and risk impact. Therefore, general prohibition might be an option to consider.

Additionally, it has been claimed that the violation of data protection and privacy as a result of the use of AI system or as a consequence of the malfunctioning of the AI system should be explicitly considered in the AI Act due to the serious impact. Simply relying on the general application of the GDPR and the ePrivacy to prevent such infringements might not be sufficiently effective. The Joint Compromise proposes a new drafting of the definition of 'serious incident' to include a 'breach of obligations under EU Law intended to protect fundamental rights' (Article 3 (44) AI Act).

[38] EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18 June 2021.

Box 5: Two sources of AI risks

In this respect a more general, non-legal commentary may be added. AI systems can be high-risk for two broad reasons: they fail to work properly (but they are potentially useful) or simply because they are put to work and they should not be used, such as for instance the potential abuse by public authorities of AI systems for surveillance purpose. Without such distinction the regulator may confuse 'the resilience that good AI systems must have, with the resistance that must be exerted towards the bad AI systems' (Floridi, 2021, p. 219). This conceptual gap, as others can spotted in the definition and scope of application will make conformity assessment harder (Floridi et al. 2018; Mokander & Floridi 2021).

b) High-risk in both AI Act and GDPR – Article 35

It might be clarified whether the categorization as high-risk under the AI Act does automatically trigger the presumption of high-risk for the purposes of the GDPR and with which consequences. Even if the initial assessment reveals that the AI system is not high-risk, a more granular impact assessment on data protection (under Article 35 GDPR) is needed considering the different uses.

c) Users and providers in the AI Act and controllers in the GDPR

In many AI systems, the data controllers, subject to the relevant obligations under the GDPR, are not the providers but the users under the AI Act. The applicable obligations differ for users under the AI Act. If the proposal of the Joint Compromise for Article 52(a) on general purpose AI system is finally adopted, the clarification of who is the relevant provider for the purposes of the AI Act in relation to an intended purpose falling under the AI Act scope is needed. The proposed drafting of the Joint Compromise does address such issue. Then, it should be maintained to prevent an unintended gap that would require interpretative effort.

d) Chapter 2 Title III AI Act

Compliance with the GDPR might be explicitly required under Chapter 2, Title III, AI Act for AI systems.

e) Article 22 GDPR

It might be dubious whether the rights enshrined in Article 22 GDPR cover AI-driven systems (automated decision making). In case, this aspect should be made explicit.

f) Remedies for individual under the AI Act

The AI Act does not specify rights and remedies available for individuals affected by AI systems. General remedies or data-specific remedies might suffice, but clarification and considered analysis are needed. The AI Act could do much more to protect consumers' rights and be much more incisive about providing measures to redress the possible harms or losses that AI systems may cause. This is the part where one may expect and welcome more improvements in the proposal.

g) Article 25 GDPR

AI systems would be subject to data protection by design and by default, where applicable, but it might not suffice. Encouraging the effective implementation of data protection principles in the design of AI systems might help to ensure consistency and guarantee proper protection under the AI Act.

h) Regulatory sandboxes - Article 53 and 54 AI Act

Despite Recital 41 of AI Act, the relationship between Article 54 AI Act and data protection regimes is unclear. GDPR provides the legal basis for 'further processing' (as referred to by Article 54 AI Act), but

the AI Act does not clarify under which criteria are the interests of data subjects taken into consideration as Articles 6(4) or 14 GDPR provides. Unless it is simply considered that Article 54 constitutes the Union law on which the 'lawful processing' is based – as Art- 6(4) GDPR clearly states. Besides, in Article 54 AI Act is not stated whether the AI systems referred therein are only be used within regulatory sandboxes.

i) Algorithmic training in the ePrivacy Regulation – and Article 10 AI Act

AI-system training, validation and test are key to ensure the development of reliable, trustworthy, safe AI. Therefore, the compatibility with purpose exception under ePrivacy Regulation is vital. Training purpose might be considered explicitly as a compatible purpose. Consent in those case and for such purpose is unfeasible. Therefore, Article 10 AI Act may be drafted accordingly.

j) M2M data processing: ePrivacy and AI Act

AI systems can frequently operate in Machine-to-Machine (M2M) environments. AI Act can apply to AI systems that process data in M2M contexts. The application of the ePrivacy Regulation to M2M communications should be clarified. Excluding M2M data processing from the scope of the ePrivacy Regulation, even if it might be covered by the AI Act, is advocated to facilitate, and promote data processing and data sharing that may drive circular and sustainable economy[39].

k) AI Act record-keeping and ePrivacy and GDPR

Article 12 of the AI Act sets out rules for logging capabilities of AI systems enabling the automatic recording of events. In complying with these logging capabilities, the high-risk AI systems should be designed and developed so as to provide at minimum the data listed in Article 12(4) AI Act. That may entail to record traffic data, access to information related to electronic communications or persona data in tracing and logging the inputs feeding the AI-driven decision-making or action. This obligation should then be put in connection with the types of communication data that the ePrivacy Directive covers as the logging purpose may interfere with the data processing rules. As regard the general material scope, the ePrivacy Directive applies when the four following conditions are met: there is an electronic communications services, offered over an electronic communication network, being the service and the network publicly available and offered in the EU. Nonetheless that, Articles 5(3) and 13 ePrivacy Directive has an expanded material scope not only covering providers of electronic communication services bat also website operators and other business. Concurrently, the data to be logged must be treated as personal data for the purposes of the GDPR. Interplay between the ePrivacy Directive and the GDPR exists. Both legal acts interact each other under a model of *lex specialis* (ePrivacy) / *lex generalis* (GDPR). Interestingly, the ePrivacy Directive 'particularises' GDPR provisions, even by limiting the general lawful processing grounds of Article 6 GDPR when ePrivacy Directive applies. In that regard, the ePrivacy Directive would act as *lex specialis* to the GDPR and, consequently, Article 5(3) ePrivacy Directive prevails over Article 6 GDPR.

5.3. AI and cybersecurity

There are several interplays between AI and cybersecurity. First, machine-learning and deep-learning techniques, might aggravate the cybersecurity risks insofar as they render cyber-attacks better targeted, more destructive, and effective, and more elusive to prevention measures as they change and

[39] Comments by the Centre for Information Policy Leadership on the Draft E-Privacy Regulation for the Purpose of the Trilogue Discussions, 29 September 2021.

adapt to new counterattacking responses. In that regard, AI increases the cybersecurity risk by expanding the cyber threats and altering the typical characteristics of cyber-attacks.

Second, on the opposite direction AI systems will enhance the effectiveness of preventive measures against cyber-attacks. AI serves as a shield against sophisticated cybersecurity breaches. The self-learning capabilities of AI will enable to rapidly accommodate the preventive and responsive actions to the changing nature of cyber-attacks.

Third, AI systems are exposed to vulnerabilities. Data-dependency, complexity, interconnectivity, and increasing autonomy due to learning capabilities expose AI systems to higher risks of hacking, unexpected outputs, malfunctioning, or undetected biases. Measures to ensure resilience, technical robustness, and cybersecurity in AI systems, and the ICT infrastructure, especially in critical and strategical sectors, are to be adopted and effectively implemented.

The three above-mentioned interactions between AI and cybersecurity lead to varied interplays between the AI Act[40] and the Cybersecurity Act[41], and the AI Act and the NIS2 Directive[42] that may reveal certain overlaps or regulatory gaps.

a) Objective/material Scope: AI Act and NIS2 Directive

The NIS2 Directive adopts a scoping strategy based on sectors, subsectors, and types of entities. As per Art. 2 NIS2 Directive, the provisions apply to public and private entities of a type referred to as essential entities in Annex I and as important entities in Annex II. Annexes I and II list types of entities (undertakings, operators, producers, market participants, providers) in a variety of sectors and subsectors classified as essential (electricity, transport, banking, financial market infrastructures, health, digital infrastructure, public administration) or important.

The AI Act approach to delimit the scope of application is, however, slightly different. The AI Act focusses on the use or purpose for which the AI system is meant. That scoping strategy is particularly illustrated by Annex III that list high-risk AI systems referred to in Art. 6(2) AI Act. Even if the listed AI systems are grouped by areas (education, employment, public services, law enforcement, migration, etc.), the selection of AI practices in the list is use/purpose-specific instead of sectoral. Additionally, the classification as high-risk AI systems intended to be used as a safety component of a product or being itself, a product covered by the Union harmonisation legislation listed in Annex II is essentially equipment-specific more than sector-specific.

Consequently, the AI Act and the NSI2 might differ in their scope of application. The AI Act requirements will only apply if an AI system included in Annex II or Annex III and therefore classified as high-risk is placed on the market, put into service, or used. Concurrently, if the user of an AI system is a public or private entity classified as an important or essential type pursuant to NSI2, such regime will apply on such grounds.

---

[40] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts, COM (2021) 206 final, Brussels, 21.4.2021.

[41] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance), PE/86/2018/REV/1, *OJ L 151, 7.6.2019, p. 15–69,*

[42] Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, COM/2020/823 final.

There are some evident connections between the use of certain AI systems in some sectors such as 'AI systems intended to be used as safety components in the management and operation of road traffic and the supply of water, gas, heating and electricity' listed in Annex III point 2 (a) of AI Act in relation to the essential entities in the subsectors of electricity, heating, or gas listed in Annex I of NIS2 Directive. But other uses and purposes of AI systems listed in Annex III of AI systems are transversal and do not necessarily fall under specific sectors.

A potential regulatory gap would only arise if an AI system covered by the AI Act is not placed on the market, put into service, or used by an essential or important entity as listed in the Annexes I and II of the NIS2 Directive.

b) Personal scope: AI Act and NIS2 Directive

The NIS2 Directive applies to public or private entities if they are included in Annexes I and II and, therefore, classified as essential or important.

The obligations provided for by the AI Act apply first to providers of high-risk AI systems. For the purposes of the AI Act, providers are defined (Art. 3(2) AI Act) as 'a natural or legal person, public authority, agency or other body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge'. Chapter 3 specifies the obligations of high-risk AI system providers (Arts. 16-23). But, in accordance with Art. 24 AI Act, such obligations do also apply to product manufacturers. Under the same Chapter 3, the AI Act also provides for obligations to importers (Art. 26), distributors (Art. 27), and even users and third parties (Arts. 28 and 29) when, under the circumstances provided for by Art. 28(1), they are considered as providers for the purposes of the AI Act.

Interestingly, the AI Act provides for obligations to 'operators' – defined in Art. 3 as 'the provider, the user, the authorised representative, the importer, and the distributor' -, whereas the NIS2 provisions apply to the public and private entities falling under the sector-based scope of application. As both positions may or may not coincide, the provisions may concurrently or alternatively apply to the market participants depending upon their status (listed entity, provider, importer, user, distributor, etc.).

c) Micro and small enterprises in AI Act and NIS2 Directive

Both legal acts take into consideration the specific interests and needs of micro and small enterprises within the meaning of Commission Recommendation 2003/361/EC, but they differ in the treatment and the extent of the exclusion. The AI Act uses the term 'small-scale provider' to describe a provider that is a micro or a small enterprise. It should be noted that the Joint Compromise proposes to replace in the AI Act the term 'small-scale provider' by 'SME provider'. Hence, the size-related criterion is relevant for providers and their obligations.

The NIS2 Directive excludes from the scope of application entities that qualify as micro and small enterprises (Art. 2(1)). Nonetheless, as explained in Recital 9 and detailed in Art. 2(2), small and micro entities fulfilling certain criteria that indicate a key role for the economies or societies or for particular sectors or types of services (trust services, top-level domain name, public administration entity, the sole provider in a Member State, potential impact on public safety), are covered by the NIS2 Directive.

Under the AI Act, small-scale providers, as named by the proposal, are not excluded from the scope of application. The provisions of the proposed Regulation apply to small-scale providers. Specific rules for small-scale providers are of two types.

First, Annex III AI Act point 5 contains a specific size-based exclusion: 'AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score' are classified as high-

risk AI system except for AI systems put into service by small scale providers for their own use. The reasons for this size-based personal exclusion are the limited scale of the impact and the available alternative on the market (Recital 37 AI Act).

Second, AI Act provides for certain measures to promote and protect innovation taking into considerations the interest of small-scale providers. That includes (Art. 55 AI Act) the access to regulatory sandboxes, awareness-raising initiatives, guidance, and advice about the implementation of the proposed Regulation, or even the proportionate reduction of fees for conformity assessment under Article 43.

Accordingly, micro, and small entities would be exempted from the obligations provided for the NIS2 Directive, except for those meeting the criteria laid down in Art. 2(2) NIS2 Directive, whereas they are neither excluded from the AI Act's scope, nor overall exempted from their obligations.

d) Critical infrastructure

The Joint Compromise proposes the inclusion of a definition of 'critical infrastructure' that would connect the AI Act with the proposed Proposal for a Directive on the resilience of critical entities (COM/2020/829 final). Adding 'critical infrastructure' in Article 5 AI Act traces a fundamental link between the AI Act and the Cybersecurity legal act insofar as it is complemented with the concept of serious incident that essentially cover disruptions related to cybersecurity resilience.

The Joint Compromise also suggests the expansion of the exceptions to the prohibited practice of real-time biometric identification in publicly accessible spaces by law enforcement authorities ('or on their behalf') precisely to cover the use of such AI system to prevent specific and substantial threats to critical infrastructure.

Thus, the AI Act's ban on certain AI purposes would not interfere, and possibly undermine the effectiveness, of the efforts to ensure the resilience of critical entities, the protection of critical infrastructure and the implementation of cybersecurity measures based on sophisticated AI systems.

e) Certification on cybersecurity: Article 42.2 AI Act in connection with Cybersecurity Act

The interplay between the AI Act requirements on cybersecurity and the Cybersecurity Act (Art. 42.2 AI Act) is the presumption that high-risk AI systems that have been certified or for which a statement of conformity has been issued under a cybersecurity scheme pursuant to the latter Regulation 2019/881 shall be presumed to follow the cybersecurity requirements set out in Article 15 AI Act.

This solution avoids duplication of compliance costs, provides legal certainty to operators, and ensures a smooth interaction of both legal acts.

f) AI Act and Regulation 2019/1020 on market surveillance

Besides, the AI Act expressly recognizes the application of the Regulation 2019/1020 on market surveillance and compliance of products[43] to AI systems covered by the AI Act with the needed adaptations: extensive concept of economic operator to include all operators of the Title III, Chapter 3, AI Act, and definition of product as to cover all AI systems falling under the scope of the AI Act.

[43] Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 (Text with EEA relevance). PE/45/2019/REV/1. *OJ L 169, 25.6.2019, p. 1–44.*

g) Sectoral safety legislation and AI Act

The interplay with existing sectoral safety legislation is ensured by integrating in the conformity assessment procedures the checking of the AI requirements (new legislative framework) and by considering the requirements of the AI Act in the adoption of relevant implementing or delegated legislation under the old approach legislation. (i.e., Art. 82 in relation to Regulation 2019/2144 on motor vehicles or the incorporation of the conformity assessment and the provider's procedural obligation into the Directive 2013/36 for credit institutions).

5.4. Other gaps or potential implementation issues

We list below gaps or potential implementation issues, extracted from chapter 2 and chapter 3:

- **Gap in the Open Data Directive**. Article 1.2 of the Open Data Directive excludes, from its scope of application, documents for which third parties hold intellectual property rights, documents excluded from access on grounds of commercial confidentiality, statistical confidentiality, and documents whose access is excluded or restricted on grounds of personal data protection. The adoption of the proposed Data Governance Act might then fill this regulatory gap that the material scope of the Open Data Directive had left unaddressed. Furthermore, there is a gap concerning B2B and B2G data sharing that might be filled in the proposed Data Act to ensure fairness in market transactions and in B2G contexts to facilitate the use of data for public interest.;
- **Gap in the current version of the Database Directive**. In the current legislative scenario, datasets can be protected as a trade secret if relevant protection conditions are met (Art. 2.1 Trade Secret Directive), by intellectual property rights if they are original (Art. 3 Database Directive). The characteristics of the data economy and the need to foster data-driven innovation require a re-evaluation of framework defined by the Database Directive. Primarily, the critical points are the following. First, the unclear status of machine-generated data and IoT data under the sui generis database right. Second, the distinction between collecting and systematizing tasks (traditional database making) and data creation activities (updating, maintenance, publication, curation);
- **P2B Regulation Gaps**. The P2B Regulation may create a regulatory gap, in that there is no obligation to share data or provide access to, but a mere duty to disclose it in the terms and conditions. So, there is no duty beyond that. It is naturally not a gap if it embodies a policy decision. The P2B Regulation leaves services unregulated and data aspects unaddressed. And in the analysis of the interplay between the DSA and the P2B Regulation, this may represent regulatory gaps for consideration. The P2B Regulation restricts its scope of application to platforms (online intermediation services providers) that enable the initiation or the completion of B2C transactions. But it should be considered whether there are sound reasons not to extend the Regulation to platforms enabling B2B transactions;
- **Implementation need for DSA**. The most challenging interplay between the DSA and the data domain is in relation to solutions adopted to minimize the information asymmetry between the market players (platforms and very large platforms) and the regulators and authorities as the main addressees and beneficiaries. Many obligations and requirements provided for by the DSA are intended to ensure data accessibility for monitoring and compliance assessment purposes. There are also other addressees of data such as auditors (Art. 28) or vetted researchers (Art. 31). This scheme the DSA is built on is highly dependent upon a solid, well-defined, and fluent infrastructure to facilitate data access with such purposes. The need to specify the data to be provided to comply with the different obligations (risk assessment,

audits, transparency reports, etc) should not be technically deemed as a regulatory gap, but it may be highlighted as an implementation need;

- **The DMA potential gaps**. Portability of data is a clear intersection between GDPR for personal data, Free Flow Regulation for non-personal data and the DMA. In assessing whether the adoption of the DMA fill or open regulatory gaps in this domain, the following considerations must be made. First, it has been argued that the scope of application defined by an exhaustive list (despite the review mechanism of Art. 17) in Article 22 might neither be complete nor future proof. The DMA applies to 'core platform services' defined as any of the following digital services: online intermediation services, online search engines, online social networking services, video-sharing platform services, number-independent interpersonal communication services, operating services, cloud computing services, advertising services. Only these services qualify. It is not a gap to fill if that represent an explicit choice. Second, the specification and the implementation of the obligations under Article 5 and, especially, under Article 6 will require further efforts to provide guidance and standards for compliance. That is not necessarily a regulatory gap, but it places the focus on the implementation stage.

5.5. Summary and regulatory taxonomy

The Table below provides a list of all the regulatory gaps identified in the previous chapters. Each identified legislative gap has been categorized according to the following regulatory taxonomy:

a) Identified in a Commission's document and already addressed under an upcoming or programmed legislative work.
b) Identified in a Commission's document, but not yet addressed under an already and upcoming or programmed legislative work.
c) Never addressed so far.

Table 2: Summary of the regulatory gaps identified

Legislation(s)	Regulatory gap	Type
AI Act	Article 5: some of the problematic practices and uses are not covered. For instance, (i) social scoring, (ii) biometric identification systems, (iii) military purpose AI systems, (iv) AI system for research.	Identified but not addressed
AI Act	The specific-purpose approach raises the question of general-purpose and multi-purpose AI systems.	Identified and addressed by Joint Compromise of November 2021
AI Act	Article 6: AI systems in insurance sector not covered in Annex II nor Annex III.	Never addressed so far
AI Act	AI regulatory sandboxing and other ongoing or future sandboxes should be better coordinated.	Never addressed so far
AI Act and Product Liability Directive	The compliance of certain obligations laid down by the AI Act may trigger (rebuttable) presumptions for the purposes of attributing liability and allocating the burden of proof.	Never addressed so far
AI Act and Product Liability Directive	It is not clear whether the high-risk category under the AI Act may impact the liability rules.	Identified but not addressed
Proposal for civil liability regime for artificial	The application of existing liability rules to damages caused by AI system is challenging. The proposal by the Parliament aimed to address this potential gap.	Identified but not addressed
Product Liability Directive	There is probably a need to update the Product Liability Directive to address AI-powered products and services.	Identified but not addressed
DSA (Article 6 and 7)	Unclear whether the deployment of a large-scale algorithm content moderation system may entail de facto general monitoring.	Never addressed so far
DSA (Article 4.1 and 5.1)	Unclear whether the poor performance of algorithm voluntary measures that fail to detect (illegal/inappropriate) content should trigger the duty to react and the resultant liability.	Never addressed so far

Legislation(s)	Regulatory gap	Type
DSA (Article 22)	To be determined the liability of the platform operator vis-à-vis the party who is relying on the trader's information.	Never addressed so far
DSA (Article 22 and 5.3)	To be better clarified cases where the consumers believe that information of the transaction was provided by platforms instead of traders. Would the platform become liable?	Never addressed so far
DSA (Article 5.3)	It is unclear whether the Article entails that the platform operator is considered contracting party, as the trader, vis-à-vis the consumer.	Never addressed so far
e-Commerce Directive	Attribution of legal effects to self-executed contracts is still unclear, with the rapid the development of AI/algorithms applications.	Never addressed so far
GDPR, AI Act, P2B Regulation, DSA	The interplay between Article 22 GDPR, the transparency requirements laid down in the AI Act, the provision on ranking of the P2B Regulation and the provisions on recommender systems for very large platform in the DSA shows that there is a need for harmonization of EU legislation on the critical topic of transparency of algorithm.	Identified but not addressed
AI Act, GDPR and ePrivacy	Relying on the general application of the GDPR and the ePrivacy to prevent violations of data protection and privacy, as a result of the use of AI system or as a consequence of the malfunctioning of the AI system, might not be sufficiently effective.	Identified and addressed by Joint Compromise of November 2021
AI Act and GDPR	Unclear whether the categorization as high-risk under the AI Act does automatically trigger the presumption of high-risk for the purposes of the GDPR and with which consequences.	Identified but not addressed
AI Act and GDPR	In many AI systems, the data controllers, subject to the relevant obligations under the GDPR, are not the providers but the users under the AI Act. The applicable obligations differ for users under the AI Act.	Identified and addressed by Joint Compromise of November 2021
GDPR	It might be dubious whether the rights enshrined in Article 22 GDPR cover AI-driven systems (automated decision making) and, if so, it should be made explicit.	Never addressed so far
AI Act and GDPR	GDPR provides for legal basis for 'further processing' (as referred to by Article 54 AI Act), but the AI Act does not clarify under which criteria the interests of data subjects are weighed.	Never addressed so far
AI Act and e-Privacy	AI-systems training purpose might be considered explicitly as a compatible purpose under the e-Privacy Regulation. Consent in those case and for such purpose is unfeasible. Therefore, Article 10 AI Act may be drafted accordingly.	Never addressed so far
AI Act and e-Privacy	AI Act can apply to AI systems that process data in Machine-to-Machine contexts. The application of the ePrivacy Regulation to M2M communications should be clarified.	Never addressed so far

Legislation(s)	Regulatory gap	Type
AI Act and NIS2 Directive	A potential regulatory gap would arise if an AI system covered by the AI Act is not placed on the market, put into service or used by an essential or important entity as listed in the Annexes I and II of the NIS2 Directive.	Never addressed so far
AI Act and NIS2 Directive	AI Act provide for obligations to 'operators', whereas the NIS2 provisions apply to the public and private entities falling under the sector-based scope of application. As both positions may or may not coincide, the provisions may concurrently or alternatively apply to the market participants depending upon their status (listed entity, provider, importer, user, distributor, etc.).	Never addressed so far
AI Act and NIS2 Directive	Micro and small entities would be exempted from the obligations provided for the NIS2 Directive, except for those meeting the criteria laid down in Art. 2(2) NIS2 Directive, whereas they are neither excluded from the AI Act's scope, nor overall exempted from their obligations.	Identified but not addressed
AI Act and Cybersecurity Act	Adding 'critical infrastructure' in Article 5 AI Act (as proposed by the Joint Compromise) creates a link between the AI Act and the Cybersecurity legal act insofar as it is complemented with the concept of serious incident that covers disruptions related to cybersecurity resilience.	Identified but not addressed
Open Data Directive	Article 1.2 of the Open Data Directive excludes, from its scope of application, documents for which third parties hold intellectual property rights, documents excluded from access on grounds of commercial confidentiality, statistical confidentiality, and documents whose access is excluded or restricted on grounds of personal data protection. The adoption of the proposed Data Governance Act might then fill this regulatory gap that the material scope of the Open Data Directive had left unaddressed.	Identified and addressed by the Data Governance Act
Database Directive	The characteristics of the data economy and the need to foster data-driven innovation require a re-evaluation of framework defined by the Database Directive.	Identified and addressed by the proposed revision of the Database Directive
P2B Regulation	The P2B Regulation may create a regulatory gap, in that there is no obligation to share data or provide access to, but a mere duty to disclose it in the terms and conditions.	Never addressed so far

6. FINAL CONSIDERATIONS AND RECOMMENDATIONS

In this conclusive chapter we first make a few final extra-legal considerations and appraisal, which are followed by six high-level and selective recommendations.

The first general consideration is that regulation of the digital domain in Europe should strike a balance between protecting fundamental rights, promoting innovation, being ambitious but at the same time coherent without adding unnecessary layers of complexity. It seems, however, that in the building of digital constitutionalism and in the search for the 'Brussels effect'[44], coherence and simplicity have been at least partially overlooked. Consider that if all the proposed acts are approved, one single company could be "controller" or "processor" under the GDPR, "data holder" under the DGA and "developer" under AI regulation. Obviously, a company may have different roles depending on the data processing done, but consistency and coherence in the terminology and in the application of the provisions should be sought. This and other aspects of the AI Act and Data Governance Act may create legal uncertainties. Making good laws can also creatively introduce new rules, as long as they are clear and intelligible, non-contradictory, stable, and possible to obey (Fuller, 1969, p. 39).

Second, the tendency of the AI Act to replicate the GDPR model could be a limitation because personal data protection and AI Regulation are fundamentally different (Papakonstantinou & De Hert, 2021a, 2021b). This is not a critique to the GDPR as such, but rather to the extent to which the AI Act attempts to mimic it. The GDPR is about a fundamental human right with respect to a single and well-identified activity: data processing. AI regulation is broader: it aims at both protecting individuals and boosting AI development and does not refer to specific activities, which poses the overambitious and unrealistic task of cataloguing AI in its entirety, given how problematic is just defining AI for legislative purposes (see Text Box 3, p. 44). Bringing all of AI under the supervision of one single authority may prove a daunting task even only because of the large volume of work needed to catalogue and monitor all possible AI uses. Furthermore, it has been noted that the AI Act has several shortcomings such as: a) enforcement regime and the risks of maximum harmonisation may pre-empt legitimate national AI policy[45]; b) it combines elements from product safety regulation, fundamental rights protection, surveillance and consumer protection law that not necessarily fits consistently together; c) the transparency provisions either add little to existing law or raise more questions than answers when their implications are considered (Veale & Zuiderveen Borgesius, 2021).

Third, as noted the AI Act '*could do much more to protect consumers' rights and be much more incisive about providing measures to redress the possible harms or losses that AI systems may cause. This is the part where one may expect and welcome more improvements in the proposal. It was one of the main recommendations made by the AI4People project: '7. Develop a redress process or mechanism to remedy or compensate for a wrong or grievance caused by AI*' (Floridi, 2021, p. 218). In reality, there are already several redress rules established at the EU level that could be leveraged also by the AI Act[46].

[44] The expression 'Brussels effect' derive from Bradford's book *The Brussels Effect. How the European Union Rules the World* (Oxford: Oxford University Press, 2020). The expression, which became very popular and by now is an idiom in policy circles, refers to the process of unilateral regulatory globalisation achieved by the European Union de facto (but not necessarily de jure) externalising its laws outside its borders through market mechanisms.

[45] While this is true for any EU legislation, for AI policy the risk of pre-empting national legislation is even greater, as the technological advancements may request a rapid national intervention before the EU legislation is adopted.

[46] See for instance "Commission welcomes confirmation of provisional agreement to strengthen collective redress in the EU" (30, June 2020: https://ec.europa.eu/commission/presscorner/detail/en/statement_20_1227).

Fourth, there are some areas of ambiguity in the interplay between the AI Act and the cyber-security legislation, in particular with the NIS2 directives both in terms of scope and of obligations for micro and small entities. The NIS2 Directive defines its scope of application based on sectors, subsectors, and types of entities. The AI Act focusses on the use or purpose for which the AI system is meant. So, the AI Act provides for obligations to 'operators', whereas the NIS2 provisions apply to the public and private entities falling under the sector-based scope of application. As both positions may or may not coincide, the provisions may concurrently or alternatively apply to the market participants depending upon their status (listed entity, provider, importer, user, distributor, etc.). Micro and small entities would be exempted from the obligations provided for the NIS2 Directive, except for those meeting the criteria laid down in Art. 2(2) NIS2 Directive, whereas they are neither excluded from the AI Act's scope, nor overall exempted from their obligations.

Fifth, when considering the legislative effort to promote B2B and B2G data sharing, it is worth recalling that such activities are not simply a matter of regulatory frameworks, but also depend on non-regulatory governance elements such as incentives, business models, culture and the need to practice and gradually build trust (see Text Box 2, p.35).

Sixth, a consideration about digital legislation and the international dimension of digital diplomacy and partnerships should also be made. As AIDA Chair Dragoş Tudorache stated: "As we prepare, at the European level, multiple and complementary pieces of legislation setting the rules of the digital world, we need to also start promoting our views, values, and rules around the world. For the EU to become a global geopolitical actor, we need to adapt our foreign policy and external action to the digital future, and a key component of this is strengthening the digital transatlantic partnership. The EU and the US are both founded on the values of freedom, human rights, democracy, and the rule of law. These values need to serve as cornerstones for the global digital future." (AIDA, 2021c, p. 3). Some of the hard regulation reviewed so far is not received immediately and intuitively well in the US and should be accompanied more by digital diplomacy. There is already some dialogue, as the European Union regularly coordinates with the US through the TTC talks[47], and Transatlantic Legislators' Dialogue (TLD)[48] works to enhance exchanges between legislators working in the European Parliament and the US Congress. However, the European digital diplomacy should improve, given that EU is likely to be the first to legislate in the digital domain on the global scene. Moreover, it has been noted that: "the EU needs to forge strong alliances worldwide with likeminded partners and overcome regulatory divergences revolving around privacy rights, data flows and taxation. Soft governance mechanisms may be more amenable to securing international consensus on AI governance than hard law approaches" (AIDA, 2021b, p. 3). In this respect, it is worth recalling the risk that the proposed Digital Governance Act may hamper transatlantic cooperation and data transfers in the same way as it happened with the Privacy shields, causing losses to European firms involved in such activities (see Text Box 1 p. 32). In fact, while the DGA proposal intends to regulate international transfers of protected data held the public sector, in practice it may however render such transfers impossible. In that respect, adequacy systems have significant drawbacks, such as the length of the process to assess the legal and judicial systems of a country and the influence of political factors.

[47] See the EU-US Trade and Technology Council Inaugural Joint Statement of 29 September 2021 available at: https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_21_4951

[48] See the European Parliament's transatlantic antiparliamentary relationship, where Members of Parliament's D-US Delegation meet their counterparts in the US House of Representatives to discuss matters of common interest, available at: https://www.europarl.europa.eu/tld/en/about/overview

These drawbacks may translate into a very limited implementation of the system that would significantly affect international data transfers.

In sum, the coherence of the regulatory system is vital to create an environment conducive to innovation, entrepreneurship, and consumer protection. Lack of coherence or excessively complex legal acts whose application and interpretation by market actors entail high costs is counterproductive. Negative externalities and unwanted effects on market access result from incoherent, inharmonious legal system. Lack of legal coherence and consistency increase complexity, which in turns is a source of barriers to market entry. These barriers are particularly dissuasive for micro-and SMEs due to the lack of capabilities to evaluate complex regulations, count on sophisticated legal advice, and re-adapt their business models to uncertain rules. Legal uncertainty related to overly complex regulations discourages innovation insofar as the cost of defining the game rules is too high for start-ups. Lack of coherence dramatically increases the cost of compliance: cost of determining which legal act is applicable and to which extent; cost of interpreting the legal provisions; cost of duplicating the compliance of requirements where the applicability is dubious to mitigate the risks of sanctions; cost of monitoring regulatory changes; cost of complying with new rules and adapting previous business models (although in many cases this cost is alleviated with transition periods in the legal acts and no-retroactivity clauses). In fragmented legal systems with a plurality of national rules potentially applicable, gaining scale is prevented. The combination of Regulations and Directives reviewed in this report may lead to a partially fragmented regulatory system. In a complex regulatory system, the legislator is in a better position to clarify the interactions between the different legal acts with clear cross-references, and undoubted referral to other legal provisions. Thus, the legislator helps private actors in the process of interpreting, applying, and complying with laws in force. The legislator has to be extremely careful in: ensuring total consistency in inter-legislation terminology and definitions; clarifying interactions among legal acts in recitals; providing specific cross-references where applicable; and providing guidance to operators/companies on the compliance of legal requirements.

Moving to high-level recommendations, our analysis of the selected relevant legal acts has revealed that the regulatory landscape is becoming highly complex. Operators in the market need to conduct a notably cost-intensive, legal-advice-dependent assessment to determine the rules applicable to the relevant activity, system, use or purpose. The interplay between the different legal acts on AI, cybersecurity, digital services and markets, and data governance is multi-fold, variegated, and in many cases dubious and confusing. Several regulatory gaps have been identified, as well as unintended interferences, overlaps or contradictions among legal instruments in different level of adoption. Based on our analysis, we propose here below six high-level recommendations:

(1) The summary table identified seven interplay gaps between the AI Act, GDPR, and ePrivacy that need to be addressed. In particular, the interplay between data protection and privacy regimes should be better clarified, since a general referral to the application of the data protection and privacy provisions is not sufficiently clear. For instance: a) relying on the general application of the GDPR and the future ePrivacy regulation framework to prevent violations of data protection and privacy, as a result of the use of AI system or as a consequence of the malfunctioning of the AI system, might not be sufficiently effective; b) in many AI systems, the data controllers, subject to the relevant obligations under the GDPR, are not the providers but the users under the AI Act. The applicable obligations differ for users under the AI Act;

(2) Clarify the compatibility of the AI Act requirements for high-risk AI systems and the requirements provided for by the cybersecurity legislation, and especially the status of micro and small entities

to avoid uncertainty on compliance requirements and possible duplication of certification and conformance costs;

(3) The AI Act currently lacks clear and well- defined mechanisms for remedies and redress to protect the rights of individuals affected by AI systems. It should add reference to collective redress mechanism already existing at EU level and specify how they would apply in the context of AI;

(4) Clarify better the liability arising from the infringement of the AI Act provisions. The compliance of certain obligations laid down by the AI Act may trigger (rebuttable) presumptions for the purposes of attributing liability and allocating the burden of proof. It is not clear whether the high-risk category under the AI Act may impact the liability rules;

(5) Revise and clarify product liability and liability rules applicable to damages caused by AI system;

(6) Coherence is needed between the AI Act and the Digital Service Act, with their respective scope of application (AI systems, algorithmic content moderation, partially automated complaint-handling, etc.).

REFERENCES

- Abraham, R., Schneider, J. & Vom Brocke, J. (2019) Data governance: A conceptual framework, structured review, and research agenda. *International Journal of Information Management*, 49: 424–438.
- AIDA (2021a). Draft Report on artificial intelligence in a digital age (2020/2266(INI)), Rapporteur Axel Voss. Brussels: European Parliament, Special Committee on Artificial Intelligence in a Digital Age (AIDA): https://www.europarl.europa.eu/doceo/document/AIDA-PR-680928_EN.pdf.
- AIDA. (2021b). AIDA Working Paper on AI and Competitiveness. Brussels: European Parliament Special Committee on Artificial Intelligence in a Digital Age (AIDA), retrieved from: https://www.europarl.europa.eu/cmsdata/237745/Working%20Paper%20on%20AI%20and%20the%20Labour%20Market.pdf.
- AIDA. (2021c). AIDA Working Paper on The External Policy Dimensions of AI. Brussels: European Parliament Special Committee on Artificial Intelligence in a Digital Age (AIDA), retrieved from: https://www.europarl.europa.eu/cmsdata/237745/Working%20Paper%20on%20AI%20and%20the%20Labour%20Market.pdf.
- Baloup, J. (2021, 10 June). The Data Governance Act: New rules for international transfers of non-personal data held by the public sector. European Law Blog,retrieved from https://europeanlawblog.eu/2021/06/10/the-data-governance-act-new-rules-for-international-transfers-of-non-personal-data-held-by-the-public-sector/.
- Bailey, K. (1994) Typologies and Taxonomies: An Introduction to Classification Techniques, Thousand Oaks: Sage Publications.
- Bertuzzi, L. (2021, 2 December). EU Council presidency pitches significant changes to AI Act proposal", *Euractiv*: https://www.euractiv.com/section/digital/news/eu-council-presidency-pitches-significant-changes-to-ai-act-proposal/.
- Bradford, A. (2020). The Brussels Effect. How the European Union Rules the World. Oxford: Oxford University Press.
- Brownsword, R. (2019). Law, Technology and Society. Reimagining the Regulatory Environment. London: Routledge.
- Buiten, M. (2019). Towards Intelligent Regulation of Artificial Intelligence. European Journal of Risk Regulation, 10(1), 41-59. https://doi.org/10.1017/err.2019.8.
- Celeste, E. (2019). Digital constitutionalism: A new systematic theorisation' (2019). *International Review of Law, Computers & Technology, 33*, 76–99.
- Chander, A. (2020). Is Data Localization a Solution for Schrems II? Journal of International Economic Law, 23(3), 771-784. https://doi.org/10.1093/jiel/jgaa024.
- Codagnone, C., Liva, G., Gunderson, L., Misuraca, G., Rebesco, E., (2021). Europe's Digital Decade and Autonomy, Publication for the committee on Industry, Research and Energy, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg.
- De Gregorio, G. (2021). The rise of digital constitutionalism in the European Union. *International Journal of Constitutional Law*. https://doi.org/10.1093/icon/moab001.

- Digital Europe. (2021). Data Flows and the Digital Decade: https://www.digitaleurope.org/wp/wp-content/uploads/2021/06/DIGITALEUROPE_Data-flows-and-the-Digital-Decade.pdf.
- European Commission. (2018). Artificial Intelligence for Europe. COM(2018) 237 final, Brussels.
- European Commission (2019). *Liability for Artificial Intelligence and Other Emerging Digital Technologies*. Expert Group on Liability and New Technologies – New Technologies Formation. Luxembourg: Publication Office of the European Union: https://op.europa.eu/en/publication-detail/-/publication/1c5e30be-1197-11ea-8c1f-01aa75ed71a1/language-en.
- European Commission. (2020a). Shaping Europe's digital future. COM(2020) 67 final, Brussels.
- European Commission. (2020b). A European Strategy to Data. COM(2020) 66 final, Brussels.
- European Commission. (2021). Commission Staff Working Document. Impact Assessment accompanying the Artificial Intelligence Act. SWD(2021) 84 final, Brussels.
- Floridi, L. (2014). *The Fourth Revolution - How the infosphere is reshaping human reality*. Oxford University Press.
- Floridi, L. (2021). The European Legislation on AI: a Brief Analysis of its Philosophical Approach. *Philosophy & Technology* , *34*, :215–222.
- Fuller, L. (1969). The Morality of Law. Yale: Yale University Press.
- HLEG B2G (2020). Towards a European strategy on business-to government data sharing for the public interest. Final report prepared by the High-Level Expert Group on Business-to-Government Data Sharing (pp.1-112) European Union.
- Kiner, C. (2020, 17 July). The Schrems II judgment of the Court of Justice and the future of data transfer regulation. European Law Blog: https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/.
- Krupi, T. (2021, 23 July). Why the proposed Artificial Intelligence Regulation does not deliver on the promise to protect individuals from harm. European Law Blog: https://europeanlawblog.eu/2021/07/23/why-the-proposed-artificial-intelligence-regulation-does-not-deliver-on-the-promise-to-protect-individuals-from-harm/.
- Malgieri, G., & Ienca, M. (2021, 7 July). The EU regulates AI but forgets to protect our mind. European Law Blog: https://europeanlawblog.eu/2021/07/07/the-eu-regulates-ai-but-forgets-to-protect-our-mind/ .
- Martens, B., & Duch-Brown, N. (2020). The Economics of Business-to-Government Data Sharing. JRC Technical Report, JRC Digital Economy Working Paper 2020-04 (pp. 1-31), European Commission.
- Micheli, M., Ponti, M., Craglia, M., & Berti Suman, A. (2020). Emerging models of data governance in the age of datafication. *Big Data & Society*, *7*(2): 1-15.
- Mokander, J., & Floridi, L. (2021). Ethics-based auditing to develop trustworthy AI. *Minds and Machines* 10.
- Papakonstantinou, V., & De Hert, P. (2021a, 8 July). EU lawmaking in the Artificial Intelligent Age: Actification, GDPR mimesis, and regulatory brutality. European Law Blog: https://europeanlawblog.eu/2021/07/08/eu-lawmaking-in-the-artificial-intelligent-age-act-ification-gdpr-mimesis-and-regulatory-brutality/ .

- Papakonstantinou, V., & De Hert, P. (2021b, 1 April). Post GDPR EU laws and their GDPR mimesis. DGA, DSA, DMA and the EU regulation of AI. European Law Blog: https://europeanlawblog.eu/2021/04/01/post-gdpr-eu-laws-and-their-gdpr-mimesis-dga-dsa-dma-and-the-eu-regulation-of-ai/ .
- Scott, J. (2014). Extraterritoriality and territorial extension in EU law. *The American Journal of Comparative Law, 62*(1), 87–126.
- Veale, M., & 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, 22(4), 97-112.

This study aims to deliver to the AIDA committee an overview of all existing and planned EU legislation in the digital field, together with an assessment of the interactions amongst these pieces of legislation.
The analysis of the interplay between the legal acts, which regulate the development, placing on the market, and use of AI systems, or other AI-related aspects, has revealed intended or inadvertent regulatory gaps that should be addressed.

This document was provided by the Policy Department for Economic, Scientific and Quality of Life Policies at the request of the special committee on Artificial Intelligence in a Digital Age (AIDA).

PE 703.345
IP/A/AIDA/2021-04

Print ISBN 978-92-846-8914-9 | doi: 10.2861/957884 | QA-06-22-057-EN-C
PDF ISBN 978-92-846-8915-6 | doi: 10.2861/73141 | QA-06-22-057-EN-N