Università Europea di Roma

Co-funded by the Erasmus+ Programme of the European Union

JEAN MONNET CHAIR IN DIGITAL TRANSFORMATION AND AI POLICY

DATA REGULATIONS AND FUNDAMENTAL RIGHTS

Course Market Law and Regulation a.y. 2023-2024

Course convenor: Professor Valeria Falce (Valeria.Falce@unier.it)

Università Europea di Roma

Co-funded by the Erasmus+ Programme of the European Union

Module 1.

Università Europea di Roma

Co-funded by the Erasmus+ Programme of the European Union

The rise of digital economy

1. What is Competition Law?

- Broadly, involves the use of legal tools to control the exercise of **market power**, in order to **protect competition** in the market.

> *Market power refers to the ability of a firm (or group of firms) to raise and maintain price above the level that would prevail under competition… The exercise of market power leads to reduced output and loss of economic welfare.* (OECD, 1993)

The rise of digital economy

Co-funded by the Erasmus+ Programme of the European Union

- **Competition** between economic actors is the **best** way to organise any market (at least in *most* instances);
- Market power held by one or more firms is not problematic in itself, but may be liable to **abuse**, which should be **prohibited**; *and*
- Competition law provides the state with a **public counterbalance to control private power**, without prohibiting private power entirely.

The rise of digital economy

Co-funded by the Erasmus+ Programme of the European Union

- **Competition** between economic actors is the **best** way to organise any market (at least in *most* instances);
- Market power held by one or more firms is not problematic in itself, but may be liable to **abuse**, which should be **prohibited**; *and*
- Competition law provides the state with a **public counterbalance to control private power**, without prohibiting private power entirely.

The rise of digital economy

Co-funded by the Erasmus+ Programme of the European Union

"Antitrust law was, as we know, invented neither by the technicians of commercial law (though they became its first specialists) nor by economists themselves (though they supplied its most solid cultural background). It was instead desired by politicians and (in Europe) by scholars attentive to the pillars of the democratic systems, who saw it as an answer (if not indeed 'the' answer) to a crucial problem for democracy: the emergence from the company or firm, as an expression of the fundamental freedom of individuals, of the opposite **phenomenon of private power**; a power devoid of legitimation and dangerously capable of infringing not just economic freedom of other private individuals, but also the balance of public decisions exposed to its domineering strength."

Amato, *Antitrust and the Bounds of Power* (1997)

The rise of digital economy

Co-funded by the Erasmus+ Programme of the European Union

- **Article 101 TFEU** (ex Art. 81 EC, Art. 85 of the EEC Treaty):
  - Prohibits anticompetitive agreements and other forms of coordination between undertakings; provides an express exemption for forms of coordination that satisfy four cumulative conditions for exemption
- **Article 102 TFEU** (ex Art. 82 EC, Art. 86 of the EEC Treaty
  - Prohibits abusive conduct by one or more undertakings holding a dominant market position
- **Regulation 139/2004**: merger control

Objectives of EU Competition Law

- **Ordoliberalism**
  - emphasis on importance of economic freedom as value in itself – protection of right to participate in economy
- **Market integration**
  - Facilitating market interpenetration
- **Efficiency** (consumer welfare)
  - “more economic approach” to EU competition law

Objectives of EU Competition Law: *GlaxoSmithKline*

"the objective assigned to Article [101 TFEU], which constitutes a fundamental provision indispensable for the achievement of the missions entrusted to the Community, in particular for the functioning of the internal market…is to prevent undertakings, by restricting competition between themselves or with third parties, from **reducing the welfare of the final consumer** of the products in question…

Case T-168/01 *GSK*, para.118

"…like other competition rules laid down in the Treaty, Article [101 TFEU] aims to protect not only the interests of competitors or of consumers, but also the **structure of the market** and, in so doing, competition as such. Consequently, for a finding that an agreement has an anti-competitive object, it is not necessary that final consumers be deprived of the advantages of effective competition in terms of supply or price…

Case C-501/06 P *GSK*, para.63

Enforcing EU Competition Law

- Centralised **public** enforcement by the European Commission
- Decentralised public enforcement by the National Competition Authorities
- Notable push to increase levels of **private** enforcement at Member State-level

The rise of digital economy

Co-funded by the Erasmus+ Programme of the European Union

- *Any abuse by one or more undertakings of a dominant position within the internal market or in a substantial part of it shall be prohibited as incompatible with the internal market in so far as it may affect trade between Member States.*

- *Such abuse may, in particular, consist in:*

(a) directly or indirectly imposing unfair purchase or selling prices or other unfair trading conditions

(b) limiting production, markets or technical development to the prejudice of consumers;

(c) applying dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage

(d) making the conclusion of contracts subject to acceptance by the other parties of supplementary obligations which, by their nature or according to commercial usage, have no connection with the subject of such contracts

Art. 102 TFEU

- *Any abuse by one or more undertakings of a dominant position within the internal market or in a substantial part of it shall be prohibited as incompatible with the internal market in so far as it may affect trade between Member States.*

- *Such abuse may, in particular, consist in:*

(a) directly or indirectly imposing unfair purchase or selling prices or other unfair trading conditions

(b) limiting production, markets or technical development to the prejudice of consumers;

(c) applying dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage

(d) making the conclusion of contracts subject to acceptance by the other parties of supplementary obligations which, by their nature or according to commercial usage, have no connection with the subject of such contracts

Goal of the provision

What are the goal of this provision:

- *consumers?*
- *competitors?*
- *competition itself?*

Co-funded by the Erasmus+ Programme of the European Union

The protective purpose of Art. 102 TFEU

Co-funded by the Erasmus+ Programme of the European Union

"Article 82 EC […] is not designed only or primarily to protect the immediate interests of individual competitors or consumers, but to protect the ***structure of the market and thus competition as such (as an institution)*** *which has already been weakened by the presence of the dominant undertaking on the market."*

(Avv. Gen. Kokott, British Airways v. Commission, Case C 95/04 P, §68)

On goals and tools

Co-funded by the Erasmus+ Programme of the European Union

Protection of competition as means to other ends.

Trust in competitive markets leading to scenario where society as a whole is better off thanks to lower prices, products available to all consumers, better quality of products and services, more innovation.

How does Art. 102 tries to achieve such goal?

1. Distinction between dominance and abuse;

- *Mere creation of dominance is not punished.*
- *Difference with US antitrust.*

2. Punishment of abuse of dominant position when such conduct ***may*** *affect trade between Member State in the internal market or a relevant sub-portion of it.*

Art. 102 TFEU

Co-funded by the Erasmus+ Programme of the European Union

- To be subject to EU Competition Law, an entity must be an '**undertaking**'.

- The concept of an undertaking includes **every entity engaged in an economic activity**, regardless of the legal status of the entity and the way in which it is financed.

Art. 102 TFEU

Co-funded by the Erasmus+ Programme of the European Union

- If two or more connected businesses (businesses within the same corporate group, multi-national companies with subsidiaries) influence the structure of a market through their conduct or through concerted strategic decisions, we might have **collective dominance**.

- In practice, a relationship between entities has been found on the basis the presence of identical conducts on the market.

- Collective dominance, as demonstrated through case law, is often associated with an **oligopoly**.

Art. 102 TFEU

Co-funded by the Erasmus+ Programme of the European Union

- The EU case law sets out a legal test that must be satisfied for collective dominance to be established (conditions are cumulative).
  - each member of the group must have the **capability of being aware of how the other members are behaving;**
  - **tacit coordination must be sustained over a period of time;**
  - it must be **proven that the potential reaction of consumers and competitors will not affect the competition** against the dominant entities.

How does the assessment proceed?

Co-funded by the Erasmus+ Programme of the European Union

1. *Definition of the relevant market;*
2. *Assessment of dominance;*
3. *Assessment of abuse:*
   - *– Presumptively abusive conduct listed in art. 102*
   - *– Presumptively abusive conduct theorized by the case law (ex. Loyalty rebates);*
   - *– Assessment on a case by case analysis of abusive conduct not expressly listed.*

How does the assessment proceed?

Co-funded by the Erasmus+ Programme of the European Union

- Before assessing dominance it is necessary to define a relevant market.
- It comprises of both a:
  - **Product Market** (a market that comprises all products and/or services which are regarded as **interchangeable or substitutable** by the consumer, by reason of the products' characteristics, their prices and their intended use).

and a

  - **Geographical Market** (which comprises the area in which the undertakings concerned are involved in the supply and demand of products or services, in which the conditions of competition are sufficiently **homogeneous** and which can be distinguished from neighboring areas because the conditions of competition are appreciably different in those area).

Again: on the difference between dominance and abuse

Dominance = situation where the competitive structure of the market is already weakened because of the very same presence of the dominant undertaking.

allowed

Abuse = subsequent moment where the dominant undertaking takes advantage of its position of strength in the market and put into practice a conduct to further increase it, to the detriment of competitors and consumers.

prohibited

Co-funded by the Erasmus+ Programme of the European Union

How does the assessment proceed?

Co-funded by the Erasmus+ Programme of the European Union

- A finding of dominance derives from the analysis of a combination of factors, the most relevant of which are:
  - constraints imposed by the existing suppliers from, and the position on the market of, **actual competitors.**
  - constraints imposed by the credible threat of future expansion by actual competitors or entry by **potential competitors.**
  - constraints imposed by the bargaining strength of the **customers (countervailing buyer power).**

How does the assessment proceed?

Co-funded by the Erasmus+ Programme of the European Union

Market share %	Assessment
100%	Monopoly or de facto monopoly
85-90%	Usually conclusive of market dominance
75%	Indicative of dominance
50%	Strong evidence of dominance
40% or more	Evidence of dominance, to be considered with other factors
25-40%	Single dominance is unlikely unless there is a fragmented market. Other factors might come into play
20%	Possibility of dominance left open but unlikely.
10%	No dominance

How does the assessment proceed?

Co-funded by the Erasmus+ Programme of the European Union

- Under a factual point of view, the "abuse" can be defined as a conduct by one or more undertakings that are not competing on the merits (on prices, quality etc.) and is likely to impair effective competition.
- There is **no legal definition of abuse** provided by the Treaty or any legislation. Article 102 was interpreted as to supervise the dominant undertaking's '**special responsibility**' not to allow its conduct to impair undistorted competition.
- There are **three forms of abuses** that could occur from anti-competitive practices: **exclusionary, exploitative;** and **single market abuse.**
- Exclusionary and exploitative abuses may be considered separately, this does not mean there is a rigid category that abuse falls into. **An overlap** of different abuses is a common occurrence.
- An effect-based analysis will normally be required for finding an abuse. However, the Commission retains the right to conclude the existence of consumer harm without carrying a detailed assessment.

Exclusionary abuses

Co-funded by the Erasmus+ Programme of the European Union

These are conducts engaged in by a dominant undertaking which are capable of **preventing competitors from entering or remaining active in a given market** .

- **Limiting production**: under Article 102(b), "limiting production, markets or technical development to the prejudice of consumers" is considered an abuse by a dominant undertaking.
- **Price discrimination**: under Article 102(c), an abuse is "applying dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage".
- **Tying**: under Article 102(d) "tying" is defined as "making the conclusion of contracts subject to acceptance by the other parties of supplementary obligations which, by their nature or according to commercial usage, have no connection with the subject of such contracts."

Exclusionary abuses

Co-funded by the Erasmus+ Programme of the European Union

- **Bundling**: arises in a situation where two products are sold together in a single package at a single price.
- **Predatory pricing**: this is the practice of dropping prices of a product below costs so that one's smaller competitors cannot cover their costs and leave the market.
- **Margin squeeze**: spread between the dominant undertaking's prices for wholesale access and its retail prices and the fact that the undertaking's wholesale products are indispensable to competition on the downstream market.
- **Granting rebates**: not an abuse in themselves, but need to analyze the effects on competition.

Exclusionary abuses

Co-funded by the Erasmus+ Programme of the European Union

- **Exclusive dealing**: an agreement whereby a customer is required to purchase all or most of a particular type of goods or services from a dominant supplier and is prevented from buying from any supplier other than the dominant firm.
- **Refusal to Supply**: happens when an undertaking which has a dominant position in the upstream market refuses to supply a new or existing customer on a downstream market on which it is also present
- **Refusal to supply intellectual property rights**: refusing to license intellectual property rights or providing interoperability information, regarded as improper exercise of intellectual property rights by a dominant firm.
- **Miscellaneous other non-pricing abuses**: conduct that does not fit within the scope of the aforementioned categories, such as sham litigation and regulatory gaming.

Exploitative abuses

Co-funded by the Erasmus+ Programme of the European Union

This type of abuse occurs when a dominant undertaking uses its position to **exploit consumers without losing them through conduct like price increase and production limitation.** Assumes barriers to entry.

- **Unfair trading conditions:** Imposition of conditions on its customers that directly harm them.
- **Excessive pricing:** price set significantly above the competitive level. The charged price must be excessive and unfair to be abusive. That is, the charged price has no reasonable relation to the economic value of the product supplied and exceeds what the dominant undertaking would have obtained in a normal and sufficiently competitive market.
- **Collecting societies:** organizations empowered with the authority to license copyrights and collects royalties from users of the copyright and distributes them to copyright owners for a fee. Abusive behavior when they discriminate undertakings from other MS.

The theory of the Special Responsibility of the dominant firm

- *"[…] a dominant undertaking is subject to certain limitations that do not apply to other undertakings in the same form. Because of the presence of the dominant undertaking, competition on the market in question is weakened. Therefore […] that undertaking has a* ***particular responsibility*** *to ensure that its conduct does not undermine effective and undistorted competition in the common market.*

(Avv. Gen. Kokott, British Airways v. Commission, Case C 95/04 P, §23)

Co-funded by the Erasmus+ Programme of the European Union

Caveat of the theory

- *"[…] A practice which would be unobjectionable under normal circumstances can be an abuse if applied by an undertaking in a dominant position".*

(Avv. Gen. Kokott, British Airways v. Commission, Case C 95 04 P, §23)

- *This caveat has historically found confirmation in the lack, within the text of the provision, of a legal mechanism to save the allegedly dominant firm.*

– No balancing mechanism such as Art. 101, 3 TFUE;

– Only the recourse to objective justification in some cases.

Objective justification

Co-funded by the Erasmus+ Programme of the European Union

- Dominant firms **may justify their behavior** either by demonstrating that their conducts are **objectively necessary** or by demonstrating that the concerned conducts **produce substantial efficiencies** which outweigh any anti-competitive effects on consumers.
- For objective justification to be applicable the conduct must be proportionate and founded on external factors (e.g. safety measures).
- To defend the conduct on efficiency grounds, **four cumulative conditions** must be satisfied:
  1. the efficiencies would have to be realized, or be likely to be realized, as a result of the conduct in question;
  2. the conduct would have to be indispensable to the realization of those efficiencies;
  3. the efficiencies would have to outweigh any negative effects on competition and consumer welfare in the affected markets; and
  4. the conduct must not eliminate all effective competition.

Further details on the doctrine of abuse

- ***Abuse as objective concept****: no prove of intent to restrict competition;*
- ***Abuse and capability to restrict competition****:*

  – The restriction of competition may be simply potential;

  – Goal of the provision: stop a conduct before it could irrevocably damage the competitive structure of the market (i.e. before actual effects have been produced).

The Discussion Paper of the EU Commission

Main goals:

- *Replacing the concept of dominance with the concept of substantial market power;*
- *Elimination of prima facie case of abuse for conduct listed in Art. 102, 2 prong;*
- *Methodology based on the effects of the conduct on the market (no presumptions);*
- *Efficiency defence for the allegedly dominant firm violating art. 102*

Guidance Paper of the EU Commission (2008)

Co-funded by the Erasmus+ Programme of the European Union

Discussion Paper	Guidance Paper
1. Replacing the concept of dominance with the concept of substantial market power;	1. Failed
2. Elimination of presumption of abuse for conducts listed in art. 102, 2 prong and those theorized by the case law.	2. Failed

Guidance Paper of the EU Commission (2008)

Co-funded by the Erasmus+ Programme of the European Union

Discussion Paper

3. Introduction of a methodology based on the effects of the conduct on the market (no presumptions);

4. Efficiency defence for the allegedly dominant firm violating Article 102

Guidance Paper

3. Introduction of the concept of anticompetitive foreclosure

   3.1. AEC test;

   3.2. Specific methodologies with economic tools for specific conduct.

4. Possibility to rebut a *prima facie* presumption of abuse with recourse to objective justifications or efficiency gains.

The notion of anti-competitive foreclosure

What is anti-competitive foreclosure?

- *"a situation where **effective access of actual or potential** competitors to supplies or markets is hampered or eliminated as a result of the conduct of the dominant undertaking whereby the dominant undertaking is likely to be in a position to profitably increase prices to the detriment of consumers".*

Guidance Paper, §19

Co-funded by the Erasmus+ Programme of the European Union

The notion of anti-competitive foreclosure

The Commission will normally intervene under Art. 102 where "[…] on the basis of cogent and convincing evidence, the ***allegedly abusive conduct is likely to lead*** *to anti competitive foreclosure" §20.*

- *Duty to provide cogent evidence, but*
- *On the likelihood to lead to anti competitive foreclose (no proof of actual foreclosure).*

Co-funded by the Erasmus+ Programme of the European Union

Factors to be taken into account

- *The position of the dominant undertaking*
- *The conditions on the relevant market*
- *The position of the dominant undertaking's competitors*
- *The position of the customers or input suppliers*
- *The extent of the allegedly abusive conduct*
- *Possible evidence of actual foreclosure*
- *Direct evidence of any exclusionary strategy*

AS EFFICIENT-COMPETITOR benchmark

Co-funded by the Erasmus+ Programme of the European Union

Always a duty to investigate on the existence of anticompetitive foreclosure

- *There may be circumstances where it is not necessary for the Commission to carry out a detailed assessment […]*

- *If it appears that the conduct can only raise obstacles to competition and that it creates no efficiencies, its anti competitive effect may be inferred §21*

→ *Prima facie case of abuse still safe!*

Co-funded by the Erasmus+ Programme of the European Union

Defenses available for the dominant firm to rebut a finding of abuse

- *Objective justification*
  - *– existence of sound reasons (normative, technical, economic) justifying the conduct*
  - *– Often exogenous to the undertaking (normative prescriptions), sometimes proper to the firm (defense of IPR)*
- *Efficiency gains*

Co-funded by the Erasmus+ Programme of the European Union

Real novelty: Efficiency gains

The Guidance Paper seems to introduce a four factor balancing exercise (echoes Article 101(3)):

– the efficiencies have been, or are likely to be, realized as a result of the conduct;

– the conduct is indispensable to the realization of those efficiencies;

– the likely efficiencies brought about by the conduct outweigh any likely negative effects on competition and consumer welfare;

– the conduct does not eliminate effective competition, by removing all or most existing sources of actual or potential competition.

Università Europea di Roma
VINCE IN BONO MALUM
Co-funded by the Erasmus+ Programme of the European Union

Prohibiting Anticompetitive Coordination (Generally)

- Anti-competitive agreements (and other forms of coordination) are prohibited by both EU and US competition law.
  - **Article 101 TFEU** (EU)
  - **§1, Sherman Act** (US)

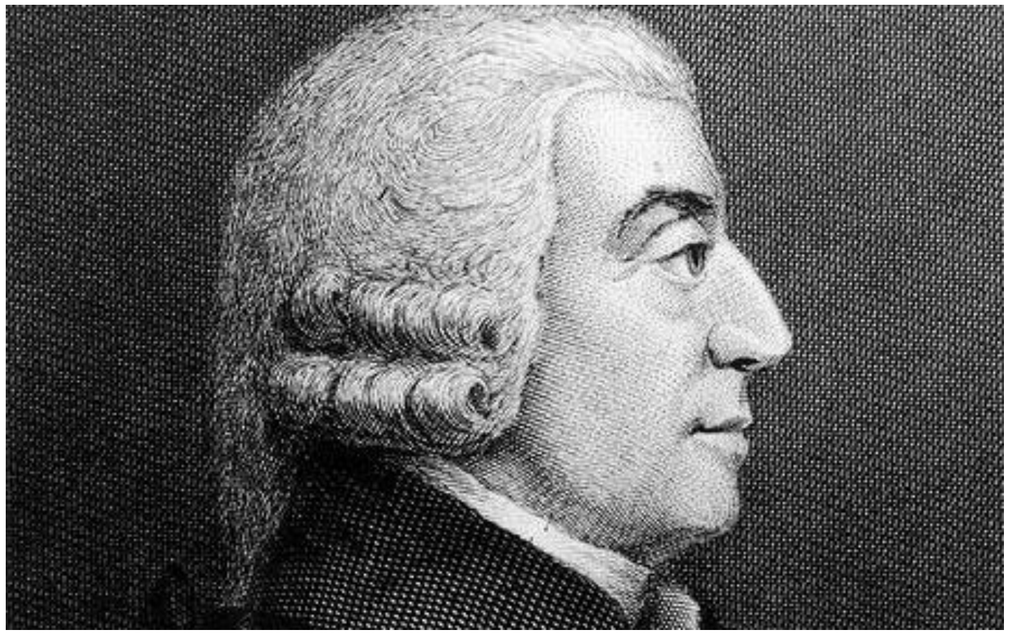
- Whilst the format of these two prohibitions varies a little, in essence both require the antitrust enforcer to establish:
  1. The existence of some form of **coordination** between two or more distinct enterprises, *with*
  2. Either an **anticompetitive** objective or an anticompetitive impact on the market in practice.

Co-funded by the Erasmus+ Programme of the European Union

Why Do We Scrutinise Agreements under Competition Law?

- **Market power** rationale: by combining, firms increase their market power and thus *influence the functioning of the market* in concert in a way that they cannot do singly

- **Conspiracy** rationale: combination of firms viewed as akin to a *morally reprehensible* group enterprise or conspiracy



"*People of the same trade seldom meet together, even for merriment and diversion, but the conversation ends in a conspiracy against the public, or in some contrivance to raise prices*."

Smith, *Wealth of Nations*, 1776

Prohibiting Anticompetitive Coordination (Generally)

Co-funded by the Erasmus+ Programme of the European Union

➢ ***Article 101 TFEU reads:***

"1. The following shall be prohibited as incompatible with the internal market: all **agreements** between **undertakings,** decisions by associations of undertakings and concerted practices which **may affect trade between Member States** and which have as their **object** or **effect** the prevention, restriction or distortion of competition within the internal market, and in particular those which:

(a) directly or indirectly fix purchase or selling prices or any other trading conditions;

(b) limit or control production, markets, technical development, or investment;

(c) share markets or sources of supply;

(d) apply dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage;

(e) make the conclusion of contracts subject to acceptance by the other parties of supplementary obligations which, by their nature or according to commercial usage, have no connection with the subject of such contracts.

2. Any agreements or decisions prohibited pursuant to this Article shall be automatically void.

3. The provisions of paragraph 1 may, however, be declared inapplicable in the case of:

- any agreement or category of agreements between undertakings,

- any decision or category of decisions by associations of undertakings,

- any concerted practice or category of concerted practices,

which contributes to improving the production or distribution of goods or to promoting technical or economic progress, while allowing consumers a fair share of the resulting benefit, and which does not:

(a) impose on the undertakings concerned restrictions which are not indispensable to the attainment of these objectives;

(b) afford such undertakings the possibility of eliminating competition in respect of a substantial part of the products in question.

EU Law: Article 101 TFEU

Article 101(1) – Prohibition

"The following shall be prohibited as incompatible with the internal market: all **agreements between undertakings**, **decisions** by associations of undertakings and **concerted practices** which may affect trade between Member States and which have as their **object** or **effect** the **prevention, restriction or distortion of competition** within the internal market…

Article 101(3) – Exception Rule

The provisions of paragraph 1 may, however, be declared inapplicable in the case of…[coordination]…which contributes to improving the production or distribution of goods or to **promoting technical or economic progress**, while **allowing consumers a fair share of the resulting benefit**, and which does not:

(a) impose on the undertakings concerned restrictions which are not **indispensable** to the attainment of these objectives;

(b) afford such undertakings the possibility of **eliminating competition** in respect of a substantial part of the products in question.

Establishing Anticompetitive Agreements

Co-funded by the Erasmus+ Programme of the European Union

Article 101 TFEU

1. **Agreement** between undertakings, **decision** by associations of undertakings or **concerted practices;**

2. Which has the **object** or **effect** of restricting competition (para.1), without sufficient countervailing **efficiency justifications** (para.3)

§1, Sherman Act

1. **Contract, combination** or **conspiracy**;

2. Which amounts to a **restraint of trade** (either because it is ***per se*** illegal, or is found to be so after a '**rule of reason**' analysis)

Coordination within the Competition Rules

- Application of Article 101(1) is premised upon some form of coordination between two or more separate undertakings: either **agreement**, **concerted practice**, or **decision of an association of undertakings**
  - cf. Article 102 TFEU, which applies to the unilateral conduct of single undertakings

- Similarly, application of §1, Sherman Act, requires the identification of some "**contract**, **combination** in the form of trust or otherwise, or **conspiracy**" involving two distinct enterprises
  - cf. §2, Sherman Act, which requires only the identification of a single legal "person" engaging in monopolisation

What is a cartel?

"A "hard core cartel" is an anticompetitive agreement, anticompetitive concerted practice, or anticompetitive arrangement by competitors to fix prices, make rigged bids (collusive tenders), establish output restrictions or quotas, or share or divide markets by allocating customers, suppliers, territories, or lines of commerce…"

OECD, *Recommendation of the Council concerning Effective Action against Hard Core Cartels* (1998)

The ‘Supreme Evil’ of Antitrust?

Co-funded by the Erasmus+ Programme of the European Union

“…CONSIDERING that hard core cartels are the most **egregious** violations of competition law and that they injure consumers in many countries by **raising prices** and **restricting supply**, thus making goods and services completely unavailable to some purchasers and unnecessarily expensive for others…

…effective action against hard core cartels is particularly important from an international perspective, because their distortion of world trade **creates market power, waste,** and **inefficiency** in countries whose markets would otherwise be competitive…”

OECD (1998)

“The **primary target** of the antitrust rules is to make certain that companies compete rather than collude. Cartels and other similar restrictive agreements distort resource allocation and encourage inefficiency”

European Commission, COM(2004) 293 final, p.6

The ‘Supreme Evil’ of Antitrust?

Co-funded by the Erasmus+ Programme of the European Union

Article 101 TFEU

- Hard core cartel offences (secret price-fixing, market-sharing, customer allocation etc.) are **object** restrictions of competition, contrary to Article 101(1)…
- …and such arrangements can, in practice, **never be justified** under Article 101(3).

§1, Sherman Act

- Hard core cartel offences are ***per se*** illegal under §1 – meaning that such arrangements are always prohibited by antitrust, regardless of any potential pro-competitive justifications for the behaviour.

Enforcement Challenges of Cartels

- Since the prohibition on hard core cartels is clear and unequivocal, most cartel behaviour these days takes place in **secret**, and cartelists often go to considerable lengths to conceal their anticompetitive arrangements

- This creates a particular challenge for anti-cartel enforcement: how can competition agencies (a) uncover the **existence** of secret cartels; and (b) gather sufficient **evidence** to mount a prosecution against such arrangements?

Co-funded by the Erasmus+ Programme of the European Union

Co-funded by the Erasmus+ Programme of the European Union

- Does competition law prove to be effective when it comes to digital markets?

- The answer relies on the analysis of the Digital Service Act Package and the Digital Single Market…

Peculiarities of digital markets

• Competition ‘for’ the market, rather than competition ‘in’ the market ➢**winner takes all**.

• **Extreme returns of scale**: marginal cost to produce digital service is close to zero ➢entry barrier.

• **Direct and indirect network effects** ➢ entry barriers.

• Role of data:

1) **’Free’ digital services**: consumers ‘pay’ the majority of digital services with personal data.

2) Data are non-rivalrous, BUT network effects limit data portability and multi-homing.

3) Data accumulation improves the services personalization ➢ competitive advantage.

• **Digital markets tend to ‘tip’ ➢dominant online platforms subject to competition law investigations**.

Common features antitrust investigations in digital markets

• Companies subject to investigations: Google, Facebook, Apple, Amazon ➢**GAFAM – Microsoft**

• **Parallel investigations by:**

1) EU Commission.
2) NCAs of the 'big' EU MS (i.e. Germany, France, Italy) + UK.

• **Categories of sanctioned conducts:**

1) 'Traditional' exclusionary abuses: tying.
2) 'New' exclusionary abuses: self-preferencing; preferential access to customers data; platform envelopment.
3) Revival of exploitative abuses: unfair trading conditions; exploitative use of personal data.

• **Limited judicial review… so far:**

1) Google Shopping: ruling EU General Court on 9th November 2021.
2) Google Android: ruling of the EU General Court on 14th September 2022.
3) Facebook (DE): preliminary ruling by EU Court of Justice (C-252/21) – ruling of the CJEU on 4th July 2023.

Shift from competition policy to sector regulation

- **Antitrust enforcement is NOT effective:**

1) NO deterrent effect: € 6 billion fine imposed by EU Commission on Google ➢small fraction of Alphabet worldwide turnover.

2) Lenghty antitrust investigations and judicial proceedings (e.g. Intel, Microsoft).

- **Political reasons**

1) DMA: preventing legislative initiatives by EU MS.

2) Europe lags behind China and the USA in digital innovation ➢ asymmetric regulation on 'big' platforms favours the entry of 'small' European platforms.

Sector regulation

• **Determines ex-ante the behaviour of firms** (e.g. price regulation, universal access obligation...) ➢ **obligations rather than prohibitions.**

• It is common in **network industries** (e.g. electricity, gas, railways, posts...):

1) Markets liberalized since 1980s, BUT still characterized by imperfect competition

2) Former State owned company remains incumbent in the market

3) Sector regulation incentivizes competition in the market (e.g. incumbent has to grant access to its network to its competitors)

• Legislation: EU Directives implemented at the national level.

• Enforcer: National Regulatory Authority (NRA) supervizes a specific network industry.

• **Sector regulation for digital platforms➢ex-ante obligations for digital platforms.**

Emergence of sector regulation of digital platforms in Europe

• EU Digital Markets Act (DMA):
a) 15.12.2020: proposal by EU Commission.
b) March 2021: political agreement between EU Parliament and Council.
c) 12.10.2022: final version DMA published on EU Official Journal.
d) 2.5.2023: DMA enters into force.

• UK Digital Market Unit (DMU):
a) April 2021: DMU established within CMA ➢advisory body, NO enforcement power.
b) UK Government has not submitted DMU bill to the House of Commons.

• Sec. 19(a) GWB:
a) 14.01.2021: German Parliament adopts 10th amendment to the GWB ➢new sec. 19(a).
b) Section 19(a) GWB: the Bundeskartellamt can prohibit conducts by **companies of 'paramount significance for competition across markets' (i.e. digital conglomerates)** without the need of proving a competition law infringement.
c) Companies subject to Sec. 19(a) GWB ➢NO remedies adopted yet:
Ø28.01.2021: Facebook.
Ø18.05.2021: Amazon.
Ø25.07.2021: Google.
Ø25.4.2023: Apple

Digital Single Market Overview

Co-funded by the Erasmus+ Programme of the European Union

What is the Digital Single Market?

- The Digital Single Market designates the 2014-2019 strategy of the European Commission for the best possible access to the online world for individuals and businesses.
- A Digital Single Market (DSM) is one in which the free movement of persons, services and capital is ensured and where the individuals and businesses can seamlessly access and engage in online activities under conditions of fair competition, and a high level of consumer and personal data protection, irrespective of their nationality or place of residence.
- The 2014-2019 Commission had identified the completion of the DSM as one of its 10 political priorities.

The Pillars

- The DSM Strategy was built on three pillars:
- Access: better access for consumers and businesses to digital goods and services across Europe;
- Environment: creating the right conditions and a level playing field for digital networks and innovative services to flourish;
- Economy & Society: maximising the growth potential of the digital economy.

EU Digital Agenda

List of Actions on the Digital Agenda (launched in 2010 under the Europe 2020 strategy) include:

- Simplifying pan-European licensing for online works
- Stakeholder debate on measures to stimulate a European online content market
- Simplifying the distribution of creative content
- Protecting intellectual property rights online

Creating a connected Digital Single Market is one of the ten priorities of the Juncker Commission.

The Digital Single Market

President Juncker
Head of European Commission

"My **first priority** will be to put policies that create growth and jobs at the centre of the policy agenda. Key to this **is creating a digital single market for consumers and businesses** – making use of the great opportunities of digital technologies which know no borders. **To do so, we will need to have the courage to break down national silos** in telecoms regulation, **in copyright** and data protection legislation, and in competition law."

Vice-President Ansip
Digital Single Market

"Take copyright, for example. Today's rules are a mess, so we need to act with some urgency. They date back to 2001. They are not suited to the digital age, for responding to new technologies, consumer behaviour and market conditions."

Commissioner Vestager
Competition

"Geo-blocking is a technical hurdle that e-commerce companies erect to make cross-border trade difficult or impossible. I have a subscription to a streamed TV package. When I am abroad I get a message saying 'Sorry, the content can only be watched from within Denmark'. Messages like this are not easy to comprehend, are they?"

Commissioner Oettinger
Digital Economy & Society

"I am quite convinced that portability on the one hand and maintaining a degree of territoriality on the other are necessary if we want to preserve cultural diversity in cinema in Europe."

EU Digital Single Market

- Communication “A Single Market for IP Rights” (24.5.2011)
- Green Paper on online distribution of audiovisual works (13.7.2011)
- Communication on content in the Digital Single Market (18.12.2012)
- Licences for Europe (5.11.2013)
- EU Copyright Review (5.12.2013)
- Digital Single Market Strategy (6.5.2015)
- Consultation of the review of the Satellite and Cable Directive (24.8.2015) and Proposed Regulation (14.9.2016)
- Communication towards a modern, more European copyright framework (9.12.2015)
- Regulation 2017/1128 on ensuring cross-border portability of online content services in the internal market (14.6.2017)
- Directive 2019/790 on Copyright in the Digital Single Market (17.4.2019)
- Directive 2019/789 on broadcasters’ online transmissions and retransmissions of television and radio programmes (17.4.2019)

Digital Single Market Strategy (6.5.2015)

- Preventing unjustified geo-blocking:
  - legislative proposals in the first half of 2016
- Competition sector inquiry on the application of competition laws to e-commerce (June 2015)
- Better access to digital content:
  - Legislative proposals before the end of 2015 to reduce differences between national copyright regimes and allow for wider online access
  - Portability of legally acquired content
  - Ensuring cross-border access to legally purchased online services while respecting the value of rights in the audiovisual sector
  - Harmonised exceptions for greater legal certainty for cross-border use of content for research and education
  - Clarifying rules on the activities of intermediaries in relation to copyright-protected content

E-commerce Sector Inquiry

The main findings of the Final Report (10 May 2017)

The report confirms that the growth of e-commerce over the last decade and, in particular, increased online price transparency and price competition, had a significant impact on companies' distribution strategies and consumer behaviour.

The final results of the sector inquiry highlight the following major market trends:

- a large proportion of manufacturers decided over the last ten years to sell their products directly to consumer through their own online retail shops, thereby competing increasingly with their distributors;
- increased use of selective distribution systems, where the products can only be sold by pre-selected authorised sellers, allows manufacturers to better control their distribution networks, in particular in terms of the quality of distribution but also price;
- increased use of contractual restrictions to better control product distribution - depending on the business model and strategy, such restrictions may take various forms, such as pricing restrictions, marketplace (platform) bans, restrictions on the use of price comparison tools and exclusion of pure online players from distribution networks.

http://ec.europa.eu/competition/antitrust/sector_inquiries_e_commerce.html

E-commerce Sector Inquiry

The main findings of the Final Report (10 May 2017)

Some of these practices may be justified, for example in order to improve the quality of product distribution, others may unduly prevent consumers from benefiting from greater product choice and lower prices in e-commerce and therefore warrant Commission action to ensure compliance with EU competition rules.

Digital content

- The results of the sector inquiry confirm that the availability of licences from content copyright holders is essential for digital content providers and a key factor that determines the level of competition in the market.
- The report points to certain licensing practices which may make it more difficult for new online business models and services to emerge. Any assessment of such licensing practices under the EU competition rules has however to consider the characteristics of the content industry.
- One of the key findings of the sector inquiry is that almost 60% of digital content providers who participated in the inquiry have contractually agreed with right holders to "geo-block". Geo-blocking prevents consumers from purchasing consumer goods and accessing digital content online from other EU Member States.

http://ec.europa.eu/competition/antitrust/sector_inquiries_e_commerce.html

Communication Towards a Modern, more European Copyright Framework (9.12.2015)

- Ensuring wider access to content across the EU:
  - EU draft regulation on cross-border portability
  - Legislative proposals in 2016 to enhance cross-border distribution of content in light of the SatCab review
  - Supporting rights holders and distributors to reach agreement on cross-border access to content including through mediation
  - Facilitating digitisation of out-of-commerce works and making them available online
  - Development of licensing hubs
- Adapting exceptions to digital and cross-border environments
  - Text and data mining, illustration for teaching, preservation by cultural heritage, "panorama"
- Achieving a well-functioning marketplace for copyright:
  - Definition of the rights of "communication to the public" and of "making available"
  - Remuneration of authors
- Providing an effective and balanced enforcement system: "follow the money"

Portability Regulation 2017/1128

Obligation on online content service providers to offer cross-border portability to the subscribers who are temporarily outside their home country

- Scope: services that are already portable in the home country; both Free and Pay services;
- ***Legal fiction that the subscriber is accessing his/her subscription from Member State of residence***
- Platform mandate
- Authentication of Member State of residence
- Temporariness
- Transition period

Entry into effect 1 April 2018

http://europa.eu/rapid/press-release_IP-15-6261_en.htm

http://europa.eu/rapid/press-release_IP-17-225_en.htm

https://ec.europa.eu/digital-single-market/en/news/regulation-cross-border-portability-online-content-services-internal-market

EU Copyright Reform Package (14.9.2016)

- Proposed regulation on online transmissions of broadcasting organisations and retransmissions of TV and radio programmes
  - Sat Cab Review
- Proposed Directive on Copyright in the Digital Single Market
  - Mandatory exceptions/out of commerce works
  - Voluntary scheme for licensing AV works on VOD platforms
  - Related right for press publishers
  - Levies for publishers
  - New duty on platforms (value gap)
  - Transparency and remuneration for authors and performers
- Proposed regulation and Directive on Marrakech Treaty

http://europa.eu/rapid/press-release_IP-16-3010_en.htm

EU Satellite and Cable Directive Review (24.8.2015)

- The SatCab Directive facilitates clearing of copyright and related rights for satellite broadcasting and cable retransmission to improve cross-border transmission and reception of broadcasting services
- Country of origin principle: rights are acquired for the EU country where the uplink takes place
- Rights cleared in one country allow broadcasters to broadcast to the whole of the EU, subject to contractual freedom
- For cable retransmission rights have to be cleared through collective management organisations

EU Satellite and Cable Directive Review (24.8.2015)

Questions for consultation:

- Are the EU rules up to date in the digital age?
- What would be the impact of extending the SatCab Directive to cover broadcasters'services over the internet (catch-up, simulcast)?

- https://ec.europa.eu/digital-single-market/en/news/eu-seeks-views-satellite-and-cable-directive

Report on the responses to the consultation:

- https://ec.europa.eu/digital-single-market/en/news/full-report-public-consultation-review-eu-satellite-and-cable-directive

EU Directive 2019/789

Co-funded by the Erasmus+ Programme of the European Union

- Vice-President for the Digital Single Market Andrus **Ansip** said: "*I am very pleased we reached yet another agreement that brings us closer to a functioning Digital Single Market. The updated broadcasting rules are a big part of the puzzle. This regulation has the potential to unlock a large amount of broadcast content across borders, benefitting the 41% of Europeans who watch TV online but also the 20 million EU citizens who were born in a different EU country from the one they live in*".

What will the directive change for the distribution of TV and radio programmes?

- **The Principle of the country of Origin (COO):** the Directive introduces the country of origin (COO) principle to facilitate the licensing of rights for certain programmes that broadcasters may wish to offer on their online services (simulcasting, catch-up services and other services that complement the main broadcast, such as previewing). Thanks to this mechanism, broadcasters will be able to make radio programmes, TV news and current affairs programmes as well as their fully financed own productions, available online in all EU countries.
- **Retransmission**: the Directive provides a mechanism to facilitate the licensing of rights in the case of retransmission of radio and TV programmes, which includes retransmission services provided over the internet under certain conditions. This measure is expected to contribute to a wider distribution of radio and TV channels.
- **Direct injection:** Direct injection is a process increasingly used by broadcasters to transmit their programmes to the public. The new rules will make sure that right holders are adequately remunerated when their works are used in programmes transmitted through direct injection. They will provide legal certainty to broadcasters and distributors involved in the process.

The final text of Article 4(1)(b) of the Geo-Blocking Regulation, approved by the European Parliament on 6 February 2018 and adopted by the Council on 27 February 2018, specifically carves out from its scope the provision of access to copyright protected works:

Article 4

Access to goods or services

1. A trader shall not apply different general conditions of access to goods or services, for reasons related to a customer's nationality, place of residence or place of establishment, where the customer seeks to:

(a) …

(b) receive electronically supplied services from the trader, ***other than services the main feature of which is the provision of access to and use of copyright protected works or other protected subject matter, including the selling of copyright protected works or protected subject matter in an intangible form***

REVIEW OF THE GEO-BLOCKING REGULATION?

Directive on Copyright in the Digital Single Market (8.4.2019)

- In September 2016 the European Commission proposed changes to copyright law including introducing a Directive on Copyright in the Digital Single Market with the intention "to create a comprehensive framework where copyrighted material, copyright holders, publishers, providers and users can all benefit from clearer rules, adapted to the digital era".
- To this end, on 13 February 2019, the European Parliament, the Council of the EU and the European Commission reached an agreement on this Directive. The Directive was subsequently passed by the European Parliament on 26 March 2019 and came into force from 2021.
- The Directive includes new copyright exceptions and limitations, rights for press publishers (and content creators) as well as regulating the position between content platforms and the respective rights holders.

Directive on Copyright in the Digital Single Market (8.4.2019)

- The Directive has caused considerable controversy with critics believing that its permissions introduce legal uncertainty and will ultimately harm the creative and digital economies.
- Some users are also concerned that content will not be as readily accessible.
- Some concessions have been made, for example, with news aggregators able to include very short pieces of news reports, although exactly what that means still must be agreed upon.
- The Directive is not enforcing upload filters on user generated content platforms and it appears that memes and gifs will be able to be shared on these platforms.
- On the other hand, the Directive's supporters believe that it will increase revenues to publishers and creators of content, which will protect and promote the publishing and creative industries.
- There is considerable uncertainty as to how the Directive will work in practice and what the commercial consequences will be for platforms, publishers/creators and users.

Directive on Copyright in the Digital Single Market (8.4.2019)

Right for publishers of press publications

- In the Directive, the new press publishers right (Article 15) gives the publishers of 'press publications', which are defined as a 'collection composed mainly of literary works,' rights to reproduce and make their works available online, for the use of their press publications by information society service providers (ISSPs). These rights will expire 2 years after the press publication is published.
- This will be relevant to online press articles by ISSPs, as Member States must provide that authors of the works, which are used in press publications, obtain an appropriate proportion of the amount that press publishers receive from the ISSPs.
- Provisionally, the use of individual words, short phrases and hyperlinks of publications will still be allowed without authorisation from press publishers.

Directive on Copyright in the Digital Single Market (8.4.2019)

Hosting user generated content

- The Directive seeks to regulate the payment received by writers and performers and the revenues enjoyed by the online platforms when they share their output. Article 17 considers that an "online content sharing provider" is communicating with the public when it allows them access to works that are protected by copyright. Sites which host user generated works will need to apply for a licence in order to present copyright protected content uploaded by users unless it complies with conditions set out in the Directive. Where no licensing agreements exist with rights holders, the platforms, under Article 17(4) will have to:
- make all efforts to obtain an agreement
- ensure the unavailability of unauthorised content where rights holders have provided the appropriate information and
- act quickly to remove any unauthorised content once notified and stop future activity.

Directive on Copyright in the Digital Single Market (8.4.2019)

Co-funded by the Erasmus+ Programme of the European Union

Hosting user generated content

- Whether the platform has observed these obligations above is determined by the principle of proportionality, the audience and types of work that users upload and the methods and costs for the platforms. At the right holder's request, platforms are obliged to provide the right holders with information regarding how they comply with their obligations set out under Article 17(4).
- For less well-established platforms, that have not been available to the public for three years and that have a turnover of less than €10 million and 5 million monthly users, they will only have to adhere to the conditions that they have made best efforts to receive authorisation and that if notified they act as quickly as possible to remove the content. If the users increase to above 5 million they will also have to make certain that notified content does not re-emerge later.
- The Directive has also set out that platforms must set out an effective complaints process that all users can access in the event that there is a dispute over removal or suspension of access to works that are uploaded. All complaints must be examined expeditiously and by human review. To further the relationship between the user and the platform, the Commission, with the help of consultations with platforms and rights holders, will discuss best practice for the parties' cooperation.

Directive on Copyright in the Digital Single Market (8.4.2019)

Co-funded by the Erasmus+ Programme of the European Union

Remuneration for authors/performers

- The new Directive gives authors and performers rights to proportionate payment on the licensing of their rights. Under the Transparency obligation in Article 19, authors have the right to detailed information about the exploitation of their work. This article sets out that Member States should ensure that the licensee to the author's work provides to the author up to-date information on the exploitation of their work at least once a year. However, the licensee can limit the burden in 'duly justified cases' where the time or administration spent on the information would be disproportionate to the amount of remuneration for the author.
- If a piece of work becomes hugely successful and the fee originally paid was too low, the Directive provides for a contract adjustment correction.
- The Directive also includes a mechanism for writers/performers to reclaim their rights when their work is not being used, although this mechanism does not apply where the lack of exploitation can be remedied easily by the author or performer.

Directive on Copyright in the Digital Single Market (8.4.2019)

Co-funded by the Erasmus+ Programme of the European Union

Exceptions and limitations

- Text and Data mining exceptions - Articles 3 and 4
- Teaching and Cultural Heritage exception - Article 5 (an online education exception for the use of online teaching), and Article 6 (a conservation and dissemination of cultural heritage exception)

Use of Out-of-commerce works (that, through a presumption of good faith, are not available through the usual channels of commerce after a "reasonable" search has been undertaken to identify whether it is publically available)

- Article 8(1) provides for Collective Management Organisations (CMOs) to be able to grant to non-CMO members, for non-commercial reasons, licences to institutions with regards to out of commerce works which reside in the collection of the institution on a permanent basis.

Appointing parties for negotiations for audio-visual works on video-on-demand (VOD)

- Where there are disputes between those who are attempting to grant licences for audio-visual works for VOD, member states are now obligated to appoint a mediator, official or impartial body to facilitate the conclusion of the licences.

Digital Single Market achievements

- Under the Juncker Commission, 30 legislative proposals on the Digital Single Market were made.

- At the end of the mandate, 28 of these legislative proposals have been agreed upon by the co-legislature.

Università Europea di Roma

Co-funded by the Erasmus+ Programme of the European Union

JEAN MONNET CHAIR IN DIGITAL TRANSFORMATION AND AI POLICY

DATA REGULATIONS AND FUNDAMENTAL RIGHTS

Course Market Law and Regulation a.y. 2023-2024

Course convenor: Professor Valeria Falce (Valeria.Falce@unier.it)

Università Europea di Roma

Co-funded by the Erasmus+ Programme of the European Union

Module 2.

Università Europea di Roma

Co-funded by the Erasmus+ Programme of the European Union

COMPETITION VS. REGULATION IN DIGITAL MARKETS

THE DIGITAL SERVICES ACT PACKAGE: THE CASE OF THE DIGITAL MARKETS ACT («DMA»)

Università Europea di Roma

Co-funded by the Erasmus+ Programme of the European Union

- Does competition law prove to be effective when it comes to digital markets?

- The answer relies on the analysis of the Digital Service Act Package…

Università Europea di Roma

Co-funded by the Erasmus+ Programme of the European Union

- **The Digital Services Act package** was presented by the European Commission in December 2020. It includes:

- the **Digital Services Act**
- the **Digital Markets Act**

Both legislative acts were quickly adopted by the Council and the European Parliament in 2022.

The new rules better govern the digital space and digital services, including social media platforms. They:

- ensure digital users have access to safe products and protect users' fundamental rights
- allow free and fair competition in the digital sectors to boost innovation and growth

Co-funded by the Erasmus+ Programme of the European Union

- In addition, a **European Data Governance Act**, which is fully in line with EU values and principles, has been proposed in the context of the European strategy for data.

- The Data Governance Act seeks to increase trust in data sharing, strengthen mechanisms to increase data availability and overcome technical obstacles to the reuse of data.

- The Data Governance Act will also support the set-up and development of common European data spaces in strategic domains, involving both private and public players, in sectors such as health, environment, energy, agriculture, mobility, finance, manufacturing, public administration and skills.

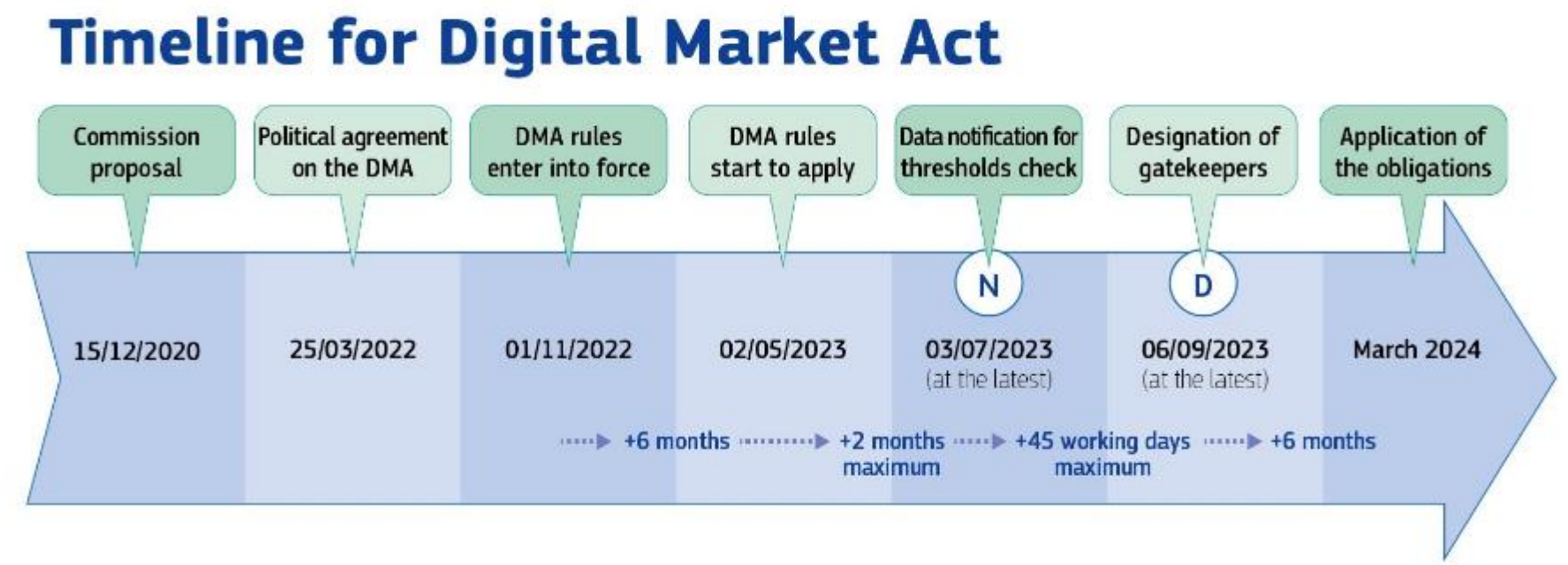
- The Data Governance entered into force on 23 June 2022 and, following a 15-month grace period, will be applicable from September 2023.

Competition vs. Regulation
The Digital Services Act Package: the case of the DMA

- In September 2022, the European Parliament and the Council adopted the Regulation on contestable and fair markets in the digital sector, better known as the Digital Markets Act ("DMA").
    - Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector [2022] OJ L265/1 (hereafter: DMA).
- The legislative process was speedy and, unusually, the final text is stricter than the one proposed by the European Commission (EC) in December 2020.
    - EC, Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector COM(2020)842 final
- With the legislative process in the rearview mirror, it is time to start looking forward to its implementation.
    - See Commission Implementing Regulation (EU) . . ./. . . of XXX on detailed arrangements for the conduct of certain proceedings by the Commission pursuant to Regulation (EU) 2022/1925 of the European Parliament and of the Council
    - On 14 April, the European Commission adopted implementing regulations detailing how the Digital Markets Act will function in practice.

Competition vs. Regulation
The Digital Services Act Package: the case of the DMA

As of 12 October 2022, the DMA was published in the Official Journal and entered into force on 1 November 2022. Before 3 July 2023, companies have to provide the Commission with information about their number of users so that the Commission can designate "gatekeepers" before 6 September. Gatekeepers will then have until March 2024 to ensure that they follow the obligations of the DMA.



Competition vs. Regulation
The Digital Services Act Package: the case of the DMA

Official Journal	**12 October 2022 (OJ L 265/1)**	
Entry into force	**1 November 2022** (20th day following publication in Official Journal)	
Application of DMA provisions	**1 November 2022** (date of entry into force)	➢ European Commission (EC) must establish a High-level group to provide with advice and expertise on implementing the DMA (Article 40). ➢ EC may adopt implementing acts, inter alia, to lay out details of notification forms and practical arrangements for cooperation and coordination between itself and the national authorities (Article 46). ➢ EC may adopt guidelines to facilitate DMA's effective implementation and enforcement (Article 47). ➢ EC may mandate European standardisation bodies to develop appropriate standards (Article 48). ➢ EC may adopt delegated acts to supplement the DMA, inter alia, by specifying the methodology for setting details of the quantitative thresholds to identify gatekeepers (Article 3(6)). ➢ Digital Markets Advisory Committee assisting EC in implementing the DMA starts work (Article 50)
	2 May 2023 (6 months after entry into force)	➢ Most provisions apply. ➢ Article 5 obligations and prohibitions (to apply directly to gatekeepers following designation): o processing and use of end users' personal data o parity clauses o anti-steering o business or end users may raise issues of non-compliance o tying o bundling o transparency concerning online advertising practices. ➢ Articles 6 and 7 obligations and prohibitions (to apply to gatekeepers subject to further specifications under Article 8(2)): o data silo o uninstalling apps and changing default settings o sideloading o self-preferencing o switching apps o interoperability o transparency concerning online advertisement performance o data portability o data access

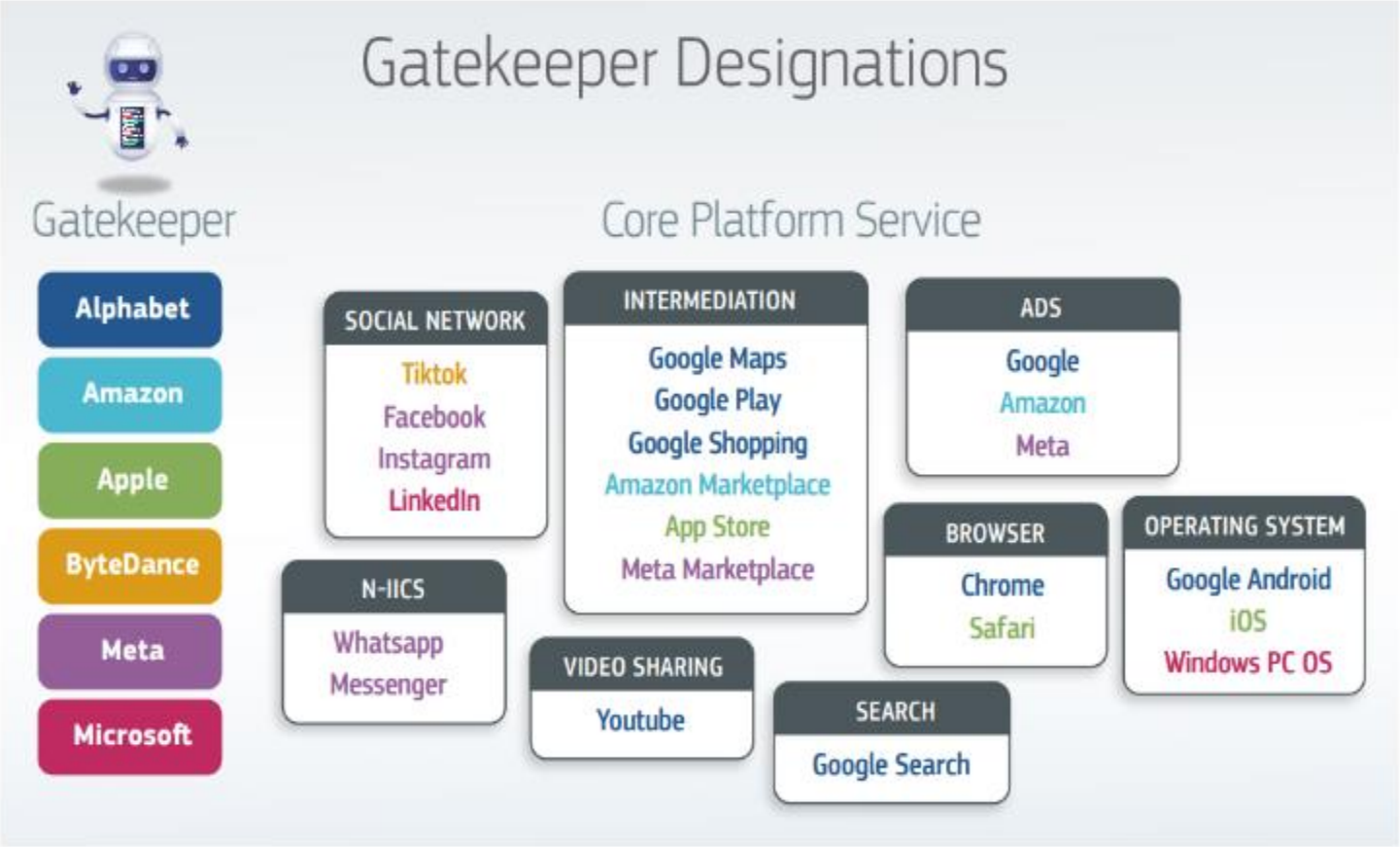
Competition vs. Regulation
The Digital Services Act Package: the case of the DMA

		○ search data access ○ access to app stores, search engines and social networking services ○ rules on terminating provision of service ○ interpersonal communications services' interoperability ○ basic functionalities' interoperability. ➢ Articles 13, 14 and 15 obligations: ○ anti-circumvention ○ information on concentrations ○ audit describing customer profiling techniques.
	25 June 2023	➢ Provisions concerning representative actions apply (Article 42). ➢ Provisions concerning whistleblowers apply (Article 43).
Gatekeeper designation procedure	**2 May 2023**	➢ Gatekeeper designation procedure starts.
	By 2 July 2023 (within 2 months of entry into application)	➢ Providers of core platform services (CPS) must self-assess whether they qualify as gatekeepers. ➢ Providers of CPS that meet the quantitative thresholds must submit a notification to the EC (Article 3(3)).
	From summer 2023	➢ EC shall designate a gatekeeper within 45 days of receiving complete information (Article 3(4)). ➢ EC may conduct market investigations to assess the evidence submitted by a CPS provider to rebut presumption of gatekeeper designation (Articles 3(5) and 17(3)). ➢ EC may conduct market investigations to designate as gatekeeper a CPS provider that does not meet the quantitative thresholds but satisfies the qualitative criteria (Articles 3(8) and 17(1)).
Compliance with obligations and prohibitions	**From 2024** (within 6 months of gatekeeper designation)	➢ Gatekeeper shall comply with obligations and prohibitions laid down in Articles 5, 6 and 7 (Article 3(10)). ➢ Gatekeeper shall provide EC with a report describing the measures implemented to ensure compliance (Article 11). ➢ Gatekeeper shall submit audit to EC describing customer profiling techniques (Article 15).
Updating obligations for gatekeepers	**From 2025**	➢ After conducting a market investigation (18 months) on its own initiative or at the request of at least three Member States, EC must submit a report and may: ○ present a legislative proposal to add new CPS or new obligations in the DMA, ○ propose a delegated act to add to existing obligations (Articles 12 and 19). ➢ Council and Parliament experts must be consulted on any delegated act, in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making.
Review clause	**3 May 2026**	➢ EC must evaluate the regulation and report to the Parliament, the Council and the European Economic and Social Committee on any amendments needed (Article 53). Evaluation must assess specifically the need to extend the Article 7 interoperability obligation to online social networking services, or to amend the provisions concerning the list of CPS, the obligations and their enforcement.

Competition vs. Regulation
The Digital Services Act Package: the case of the DMA

1. The EU Commission has made it in time to designate the economic operators which will be the targets of the DMA. On the 6th of September, the EC issued a press release detailing the different actions it had endeavoured since seven different undertakings had notified their potential status as gatekeepers on 4 July (the undertakings being Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft and Samsung).
2. Although a few designations were cut clear from the DMA's drafting, the decisions of the Commission have been anything but predictable.
3. From the seven initial notifications, **the Commission has finally designated six different gatekeepers (Alphabet, Amazon, Apple, ByteDance, Meta and Microsoft).** For the moment, **Samsung has been left adrift and has not fallen under the scope of designation** and the possibilities abound relating to the possible pathways that the South Korean company may have achieved that.

Competition vs. Regulation
The Digital Services Act Package: the case of the DMA



Competition vs. Regulation
The Digital Services Act Package: the case of the DMA

1. In parallel to the completed designations, the Commission will investigate for four different of the gatekeeper's services whether they qualify as gateways or not. From the EC's press release, it seems like Microsoft and Apple decided to rebut the presumption of falling within the scope of the DMA (Article 3(5) DMA).

1. Before the rebuttal of the presumption, the Commission can determine whether the arguments put forward by the undertakings are sufficiently substantiated to call into question the application of the presumption. If it considers that to be the case, then the Commission is bound to trigger the market investigation procedure contained under Article 17(3) DMA**. This was the case for Microsoft's online search engine (Bing), web browser (Edge) and online advertising services (Microsoft Advertising) as well as for Apple's number-independent interpersonal communications service (iMessages).**

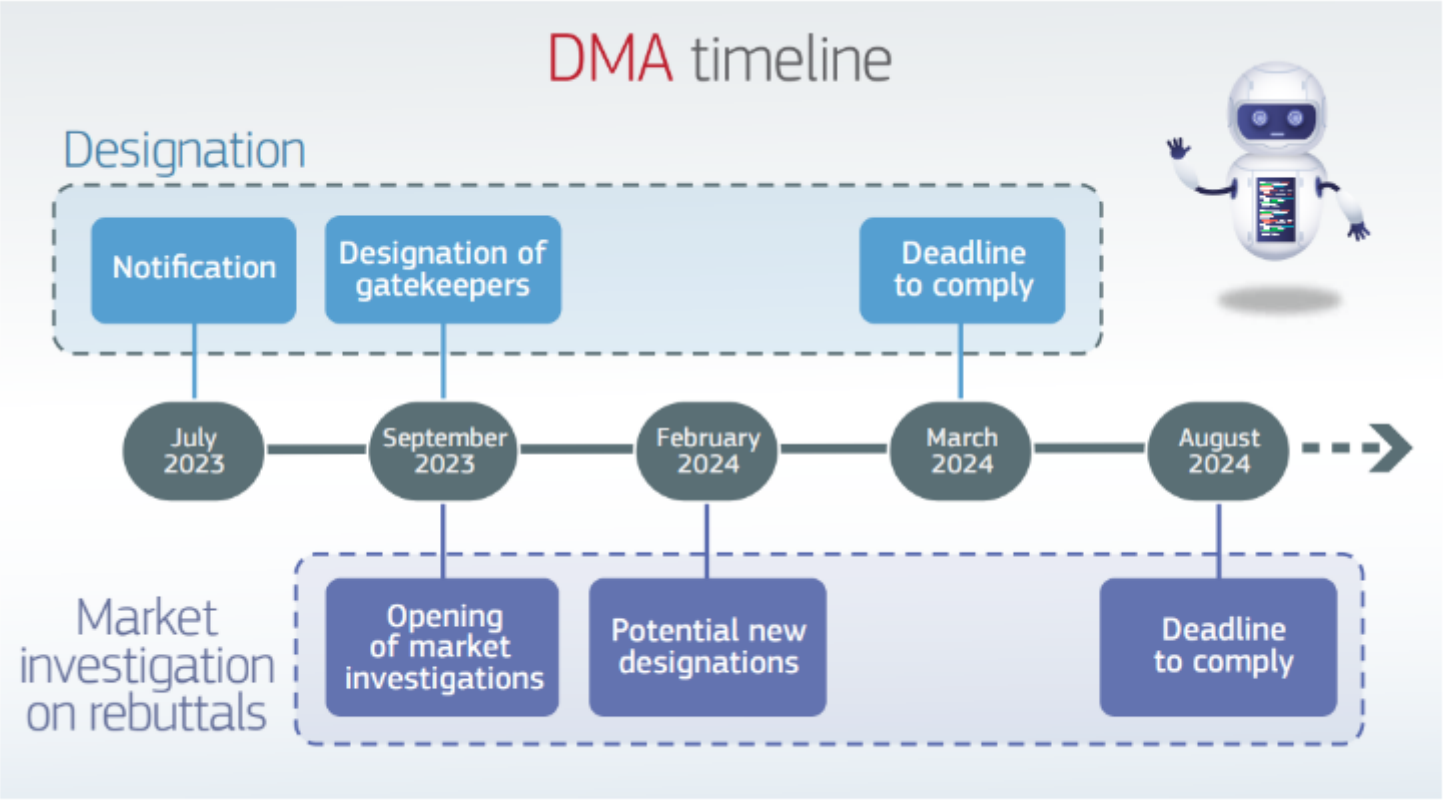
Competition vs. Regulation
The Digital Services Act Package: the case of the DMA

1. In addition, the Commission has opened a market investigation to further assess whether **Apple's iPadOS should be designated as gatekeeper, despite not meeting the thresholds**. Under the DMA, this investigation should be completed within a maximum of 12 months.

2. In addition, the Commission has concluded that, **although Gmail, Outlook.com and Samsung Internet Browser meet the thresholds under the DMA to qualify as a gatekeeper**, Alphabet, Microsoft and Samsung provided sufficiently justified arguments showing that these services do not qualify as gateways for the respective core platform services. Therefore, the Commission decided not to designate Gmail, Outlook.com and Samsung Internet Browser as core platform services. It follows that Samsung is not designated as gatekeeper with respect to any core platform service.

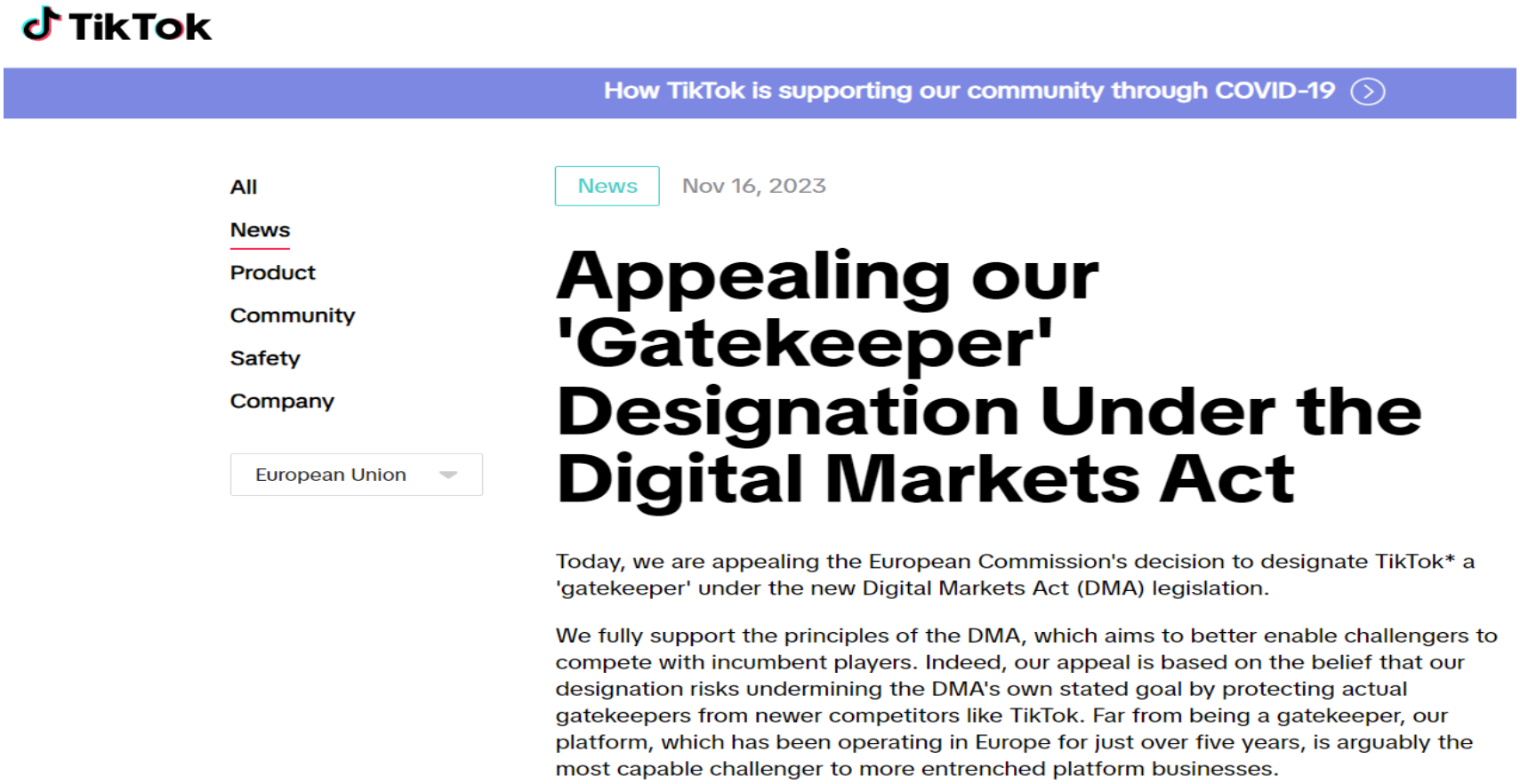
3. **Following their designation, gatekeepers now have six months to comply with the full list of do's and don'ts under the DMA.**

Competition vs. Regulation
The Digital Services Act Package: the case of the DMA



Competition vs. Regulation
The Digital Services Act Package: the case of the DMA

1. But very recently…



Competition vs. Regulation
The Digital Services Act Package: the case of the DMA

1. But very recently…

REUTERS® World Business Markets Sustainability Legal Breakingviews Technology Investigations

Technology

Meta appeals against EU gatekeeper status for Messenger, Marketplace

By **Supantha Mukherjee** and **Foo Yun Chee**

November 15, 2023 7:12 PM GMT+1 · Updated 18 hours ago

Competition vs. Regulation
The Digital Services Act Package: the case of the DMA

1. But very recently…

CPI COMPETITION POLICY INTERNATIONAL
A PYMNTS Company

Pricing News Columns Blog o' Blogs Antitrust Chronicles TechREG Chronicles

Apple to Challenge EU's Digital Markets Act, Contests App Store Inclusion

BY **CPI** | NOVEMBER 12, 2023

Competition vs. Regulation
The Digital Services Act Package: the case of the DMA

1. On 25 March 2024, the Commission announced that it had opened non-compliance investigations under the DMA into three of the companies that have been designated as gatekeepers, **namely Alphabet, Apple, and Meta**. These investigations concern various issues, including rules on steering in app stores, choice screens for browsers, self-preferencing in general search, and data combination.

2. Moreover, the Commission announced that it has **taken investigatory steps relating to Apple's new fee structure for alternative app stores and Amazon's ranking practices on its marketplace**. In practice, this means that the Commission has made use of the tools it has under the DMA (Article 20(2) and following), such as requests for information and/or interviews, to gather the information it needs with a view to determining whether to launch non-compliance proceedings.

Competition vs. Regulation
The Digital Services Act Package: the case of the DMA

1. The Commission's investigations were launched on the back of the gatekeepers' compliance reports. Concretely, following their designation in September 2023, **designated undertakings had six months (i.e., until 7 March 2024) to ensure and demonstrate compliance with the obligations and prohibitions established in the DMA (Article 8(1))**. To enable the Commission to monitor compliance with the DMA, gatekeepers are required to (a) provide it with a report describing in a detailed and transparent manner the measures they implemented, and (b) publish a non-confidential summary of those reports (Article 11).

2. **Gatekeepers made available to the Commission and the public the changes they made to adjust to the new regulatory regime introduced by the DMA**. However, whether the measures under scrutiny "effectively" comply with the DMA is not obvious.

Competition vs. Regulation
The Digital Services Act Package: the case of the DMA

1. **The idea underlying these initiatives is that competition law is too narrow, either by design or through judicial interpretation (in particular in the United States), which has led to under-enforcement, especially in the digital economy. Accordingly, the new laws are supposed to recalibrate enforcement.**

- The DMA is explicitly grounded on the assumption that competition law alone is unfit to effectively address challenges and systemic problems posed by the platform economy.
- Indeed, the scope of antitrust rules is limited to certain instances of market power (e.g., dominance on specific markets) and of anti-competitive behaviour.
- Furthermore, its enforcement occurs ex post and requires an extensive investigation of often very complex facts on a case-by-case basis. Moreover, it does not address, or does not address effectively, the challenges to the well-functioning of the market posed by the conduct of gatekeepers, which are not necessarily dominant in competition law terms.

Competition vs. Regulation
The Digital Service Act Package: the case of the DMA

1. **The idea underlying these initiatives is that competition law is too narrow, either by design or through judicial interpretation (in particular in the United States), which has led to under-enforcement, especially in the digital economy. Accordingly, the new laws are supposed to recalibrate enforcement.**

- As a result, a regulatory intervention is invoked to complement traditional antitrust rules by introducing a set of ex ante obligations for online platforms designated as gatekeepers, and dispensing enforcers from defining relevant markets, proving dominance, and measuring market effects.

Competition vs. Regulation
The Digital Service Act Package: the case of the DMA

2. The declared aim of the DMA is to protect a different legal interest from those of antitrust rules, notably it pursues an objective that is different from that of protecting undistorted competition on any given market, as defined in competition law terms, which is to ensure that markets where gatekeepers are present are, and remain, contestable and fair, independently from the actual, likely or presumed effects of the conduct of a given gatekeeper (DMA, Recital 11).

- Accordingly, the relevant legal basis is represented by Article 114 TFEU, rather than Article 103 TFEU, which is intended for the implementation of antitrust provisions pursuant to Articles 101 and 102 TFEU.

Competition vs. Regulation
The Digital Service Act Package: the case of the DMA

3. The DMA's stated objective is "to ensure that markets where gatekeepers are present are and remain contestable and fair." (DMA, Recital 11)

- Those goals of contestability and fairness are not explicitly defined.
- The clearest articulation of contestability is that it relates to "the ability of undertakings to effectively overcome barriers to entry and expansion and challenge the gatekeeper on the merits of their products and services." (DMA, Recital 32)
- The idea is that the features of platform markets (network effects, strong economies of scale, benefits from data) currently limit the contestability of gatekeeper positions and that the DMA should lower the barriers to entry, in particular to the benefit of new challengers.

Competition vs. Regulation
The Digital Service Act Package: the case of the DMA

3. The DMA's stated objective is "to ensure that markets where gatekeepers are present are and remain contestable and fair." (DMA, Recital 11)

- Those goals of contestability and fairness are not explicitly defined.
- Fairness, by contrast, relates to "an imbalance between the rights and obligations of business users where the gatekeeper obtains a disproportionate advantage." (DMA, Recital 33)
- The idea is that gatekeepers use their superior bargaining position to appropriate the efforts of business users, either directly (by exploiting them) or indirectly (by excluding them from the market, especially when they compete with services provided by the gatekeeper).

Competition vs. Regulation
The Digital Service Act Package: the case of the DMA

4. In other words, the DMA is aimed at making room for innovation by smaller players and letting such players reap the benefits from their innovative (and other) efforts.

- In short, the DMA tries to distinguish itself from EU competition law but only succeeds in doing so to a limited extent. Fairness goes back to intra-platform exclusion and exploitation, while contestability refers to inter-platform competition (although promoting and not simply protecting such competition goes beyond competition law).
- At the same time, the DMA's reason for adoption (as a response to competition law's perceived ineffectiveness) and more prescriptive nature are reminiscent of sectoral regulation. It is thus not necessary to fit the DMA into a competition law straitjacket, but it is justified to use competition law as a reference point. Substantive or procedural departures from competition law may very well be justified when the law is not attaining its goal of undistorted competition (and its corollary, consumer welfare).

Competition vs. Regulation
The Digital Service Act Package: the case of the DMA

In addition to sketching this global push for platform regulation, it is important to situate the DMA within the wider EU effort to regulate various aspects of digital markets, focusing on the instruments that it interacts with.

First, the DMA is part of a package that also includes the **Digital Services Act (DSA)**, which focuses on the accountability of online platforms regarding illegal and harmful content.

Second, the DMA goes a step further than the **Platform-to-Business (P2B) Regulation** of 2019, which focused on introducing transparency in the relation between platforms and their business users.

Third, the DMA shares a concern for data protection with **the General Data Protection Regulation (GDPR)**, and even strengthens it on certain fronts.

Fourth, the DMA's contestability goal is reminiscent of the pluralism pursued by the **Audiovisual Media Services Directive**.

Finally, though not adopted with the digital economy in mind, the **Unfair Commercial Practices Directive** has a similar focus on fairness and also includes a "blacklist" of banned practices.

Competition vs. Regulation
The Digital Service Act Package: the case of the DMA

- **The Gatekeeper concept**
- The DMA's scope is determined by the concept of "gatekeeper".
- "Gatekeeper" is defined as an undertaking providing core platform services (CPS) that is designated as gatekeeper according to certain criteria (DMA, art. 2(1)).
- It makes sense to look at the two components – CPS and gatekeeper status – separately.
- CPS are defined by reference to a close list of types of online platforms (DMA, art. 2(2)).

Competition vs. Regulation
The Digital Service Act Package: the case of the DMA

- **The Gatekeeper concept**
- They include the usual suspects, including intermediation services (e.g., marketplaces and app stores), search engines, social networks, OS, and advertising (intermediation) services, as well as some less obvious choices (i.e., video-sharing services, number-independent interpersonal communication services (NIICS), web browsers, virtual assistants and cloud computing services).
- The DMA defines each of these CPS separately, often in reference to other EU regulation. The idea is that CPS constitute gateways in the digital economy, with the capacity to affect a large number of end-users and businesses, which is not a problem in itself. Sufficiently serious concerns around fairness and contestability only arise when a CPS becomes an unavoidable gateway – in other words, a gatekeeper.

Competition vs. Regulation
The Digital Service Act Package: the case of the DMA

- **The Gatekeeper concept**
- Gatekeeper status is dependent on three qualitative criteria. For each criterion, there are quantitative thresholds; when those are met, the qualitative criterion is presumed to be fulfilled.
- According to those qualitative criteria and corresponding quantitative thresholds, an undertaking qualifies as gatekeeper if

(a) it has a significant impact on the internal market: this is the case where it achieved an annual EU turnover above €7.5B in each of the last three financial years, or where its average market cap amounted to at least €75B in the last financial year, and it provides the same CPS in at least three Member States;

(b) the CPS it provides is an important gateway for business users to reach end-users: this is the case where in the last financial year, the CPS had at least 45M monthly active end-users established or located in the EU and at least 10,000 yearly active business users established in the EU;

(c) it enjoys an entrenched and durable position: this is the case where the thresholds of (b) were met in each of the last three financial years.

Competition vs. Regulation
The Digital Service Act Package: the case of the DMA

- **The Gatekeeper concept**

Potential Gatekeeper	Core Platform Services			
	Intermediation	Search	Social	Video-sharing
Google (Alphabet)	Play Store	Google Search	—	YouTube
Apple	App Store	—	—	—
Microsoft	Microsoft Store	—	LinkedIn	—
Amazon	Amazon Marketplace	—	—	—
Facebook (Meta)	Facebook Marketplace	—	Facebook Blue, Instagram	Facebook Watch, IGTV/ Reels
	NIICS[120]	OS	Browser	Advertising[121]
Google (Alphabet)	Gmail, Messages, Google Meet	Android (Auto)	Chrome	Related to CPS (search), intermediation
Apple	Mail/iCloud, iMessage	iOS (CarPlay), macOS	Safari	Related to CPS (intermediation)
Microsoft	Outlook, Teams	Windows	Edge	Related to CPS (social)
Amazon	—	—	—	Related to CPS (intermediation)
Facebook (Meta)	Messenger, WhatsApp, Instagram	—	—	Related to CPS (social), intermediation

Competition vs. Regulation
The Digital Service Act Package: the case of the DMA

- **The DMA Obligations**

- The DMA contains a list of 22 prohibitions and obligations included in three separate groups:
  - Article 5 enumerates 9 items, mostly prohibitions, which are supposed to be self-explanatory and self-executing;
  - Article 6 lists 12 items, mostly obligations, which may require additional specificity by the Commission; and
  - Finally, Article 7 adds a horizontal interoperability obligation among communications applications, which requires a phased implementation given its complexity.

Competition vs. Regulation
The Digital Service Act Package: the case of the DMA

- **The DMA Obligations**
- Even if the DMA itself does not cluster these prohibitions and obligations, it can be useful to group them around four categories. This clustering of obligations allows the link between the objectives of the DMA and its substantive part, as well as the relationship between the individual obligations, to be made more explicit.

    1. **Preventing anti-competitive leverage from one service to another**. This category includes the prohibition of tying one regulated core platform service (CPS) to another regulated CPS, or tying one CPS to identity or payment services, as well as the prohibition of specific discriminatory or self-preferencing practices.

Competition vs. Regulation
The Digital Service Act Package: the case of the DMA

- **The DMA Obligations**

2. **Facilitating business and end users switching and multi-homing**, thereby reducing entry barriers arising from user demand. This category includes the prohibition of Most Favoured Nation clauses, anti-steering and anti- disintermediating clauses, as well as disproportionate conditions to terminate services. It also includes the obligation to ensure that it is easy to install applications or change defaults, as well as to port data outside of core platform services.

3. **Opening platforms and data**, thereby reducing supply-side entry barriers and facilitating the entry of complementors, competitors and disruptors. This category includes horizontal and vertical interoperability obligations, FRAND access to app stores, search engines and social networks, and data access for business users as well as data sharing among search engines on FRAND terms.

Competition vs. Regulation
The Digital Service Act Package: the case of the DMA

- **The DMA Obligations**

> 4. **Increasing transparency** in the opaque and concentrated online advertisement value chain. This more specific category includes transparency obligations on price and performance indicators, which are to the benefit of advertisers and publishers.

The first category includes mostly prohibitions that are inspired by competition cases and are hence drafted in a relatively detailed manner. The second and – especially – the third categories include mostly obligations couched in more general terms and sometimes going beyond what could be imposed by way of competition law remedies. Each of these categories points to different aspects of contestability and fairness, as defined above. When the obligations are read together with the corresponding recitals, it becomes apparent that almost all of them relate to contestability, and many of them to fairness as well. The justifications set out in the recitals often blend contestability and fairness, underlining that they are indeed linked and that contestability seems to be the leading objective.

Competition vs. Regulation
The Digital Service Act Package: the case of the DMA

- **The DMA Obligations**

It is also possible to divide most of the DMA's obligations in just two groups: negative and positive. Although there are too many exceptions to speak of a "rule," negative obligations tend to correspond to the DMA's fairness goal, that is, to protect intra-platform competition, while positive obligations are more likely to relate to contestability, that is, to promote inter-platform competition. Let us examine the two groups.

Negative obligations or "don'ts" - proscriptive rules - are the prohibitions typical to competition law. Enforcement of such obligations results in injunctions or cease-and-desist orders ("reactive" remedies). In the DMA's text, negative obligations can be recognized from their wording, with "shall not" or "shall refrain" being giveaways (although language is bendable and thus not always helpful to unearth the nature of the obligation). An example of a negative obligation is the prohibition of antisteering measures, which prevent business users from communicating and promoting offers to end-users acquired via the CPS. These negative obligations tend to relate to the DMA's fairness goal, that is, seek to prevent gatekeepers from excluding or exploiting (business) users of its CPS.

Competition vs. Regulation
The Digital Service Act Package: the case of the DMA

- **The DMA Obligations**

Positive obligations or "dos" - prescriptive rules - are less usual for competition law. When it comes to remedies, a simple injunction does not suffice; rather, positive obligations require the enforcer to specify a desired course of action in greater detail ("proactive" remedies). Such remedies are not unheard of in competition law but are usually avoided given that they come with a greater need for design expertise and consistent monitoring. It is therefore only logical that most of the DMA's positive obligations are those that are "susceptible of being further specified" (Article 6). The text hints at the nature of such obligations with phrases like "shall allow (and technically enable)" and "shall provide." A good example is the obligation of gatekeeper search engines to provide third parties with access to ranking, query, click, and view data on FRAND terms. Positive obligations tend to relate to the DMA's contestability goal, that is, the promotion of inter-platform competition.

Competition vs. Regulation
The Digital Service Act Package: the case of the DMA

- **The DMA Obligations**

Article	Obligation[170]	Goal	Precedents
Negative obligations			
5(2)(a)	Not process personal data from third parties	Inter-platform	Bundeskartellamt (BKA), *Facebook*[171] Competition and Markets Authority (CMA), Digital advertising market study[172]
5(2)(b), (d)	Not combine personal data from CPS with data from third parties and other services gatekeeper	Inter-platform	BKA, *Facebook* and *Facebook/Oculus*[173] Autorità Garante della Concorrenza e del Mercato (AGCM), *Facebook*[174] CMA, Digital advertising market study
5(2)(c)	Not cross-use personal data from CPS in other services gatekeeper	—	Belgian Competition Authority, *Nationale Loterij*[175] Autorité de la concurrence (AdlC), *Engie*[176] AGCM, *Enel*[177]
5(3)	Not impose narrow and wide most favored nation clauses (MFNs)	Respectively intra- and inter-platform	EC, *E-books [Apple]*[178] and *E-book MFNs (Amazon)*[179] CMA, *Amazon*[180] BKA, *Amazon*,[181] *HRS*,[182] *Booking*,[183] *Verivox*[184] and *Amazon*[185] AdlC, AGCM and Konkurrensverket, *Booking*[186] Paris Commercial Court, *Amazon*[187]
5(4), 5(5)	Not impose anti-steering and supporting measures (cross-platform access to content)	Intra-platform	EC, *Apple App Store Practices*[188] Dutch Competition Authority (ACM), *Apple*[189]
5(7), 5(8)	Not require use of certain secondary services or registration with other CPS	Intra-platform	ID service: BKA, *Facebook/Oculus* Web browser: CMA, Mobile ecosystems market study[190] and subsequent Mobile browsers market investigation[191] Payment: EC, *Apple App Store Practices*; ACM, *Apple* and CMA, Mobile ecosystems market study Other CPS: EC, *Google Android*[192] and *Facebook Marketplace*[193]
6(2)	Not use business users' data to compete with them	Intra-platform	EC, *Amazon Marketplace*[194] and *Facebook Marketplace*
6(5)	Not self-preference in ranking	Intra-platform	EC, *Google Search (Shopping)*[195] and *Amazon Buy Box*[196] AGCM, *Amazon*[197]
6(6)	Not restrict switching between secondary services	Intra-platform	—

Competition vs. Regulation
The Digital Service Act Package: the case of the DMA

- **The DMA Obligations**

Positive obligations			
6(3)	Allow un-installation and prompt default selection (search, browser, assistant)	Intra-platform	EC, *Microsoft I* (tying abuse),[198] *Microsoft II*[199] and *Google Android* CMA, Mobile ecosystems market study
6(4)	Allow installation and default selection of third-party apps, app stores	Inter-platform	—
6(7)	Allow equal interoperability with hardware and software features	Intra-platform	EC, *Microsoft I* (refusal to supply abuse) and *Apple Mobile Payments*[200] ACM, Big Techs in the payment system (report),[201] see also the subsequent investigation[202] AdIC, *Google (online advertising)*[203] AGCM, *Android Auto*[204] See also the German "Lex Apple Pay"[205]
6(9)	Provide end-users data portability	Inter-platform	—, but see GDPR, art 20
6(10)	Provide business users access to self-generated data	Intra-platform	—
6(11)	Provide FRAND access to search data	Inter-platform	—, but see CMA, Retail banking market investigation[206] and PSD2[207]

Article	Obligation[170]	Goal	Precedents
6(12)	Provide FRAND access to app stores, search and social	Intra-platform	App stores: Paris Commercial Court, *Google*[208]; ACM, Mobile app stores market study[209] and CMA, Mobile ecosystems market study Search: EC, *Google Search (Shopping)*
6(13)	Maintain proportionate CPS termination terms	Inter-platform	—
7	interoperability of NIICS	Inter-platform	—, but see Communications Code[210]

Competition vs. Regulation
The Digital Service Act Package: the case of the DMA

- **The DMA Obligations**

Positive obligations or "dos" - prescriptive rules - are less usual for competition law. When it comes to remedies, a simple injunction does not suffice; rather, positive obligations require the enforcer to specify a desired course of action in greater detail ("proactive" remedies). Such remedies are not unheard of in competition law but are usually avoided given that they come with a greater need for design expertise and consistent monitoring. It is therefore only logical that most of the DMA's positive obligations are those that are "susceptible of being further specified" (Article 6). The text hints at the nature of such obligations with phrases like "shall allow (and technically enable)" and "shall provide." A good example is the obligation of gatekeeper search engines to provide third parties with access to ranking, query, click, and view data on FRAND terms. Positive obligations tend to relate to the DMA's contestability goal, that is, the promotion of inter-platform competition.

Università Europea di Roma

Co-funded by the Erasmus+ Programme of the European Union

COMPETITION VS. REGULATION IN DIGITAL MARKETS

THE DIGITAL SERVICES ACT PACKAGE: THE CASE OF THE DIGITAL SERVICES ACT («DSA»)

Competition vs. Regulation
The Digital Service Act Package: the case of the DSA

- The DSA has been published in the Official Journal as of 27 October 2022 and came into force on 16 November 2022. The DSA will be directly applicable across the EU and will apply fifteen months or from 1 January 2024, whichever comes later, after entry into force.

- For online platforms, they must publish their number of active users by 17 February 2023. If the platform or a search engine has more than 45 million users (10% of the population in Europe), the Commission will designate the service as a very large online platform or a very large online search engine. These services will have 4 months to comply with the obligations of the DSA, which includes carrying out and providing the Commission with their first annual risk assessment. EU Member States will have to appoint Digital Services Coordinators by 17 February 2024, when also platforms with less than 45 million active users have to comply with all the DSA rules.

Competition vs. Regulation
The Digital Service Act Package: the case of the DSA

- The **DSA introduces a new regulatory framework for online platforms**. Its goal is to encourage them to fight objectionable content while respecting users' fundamental rights.
- The DSA **updates and complements the provisions of Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the internal market** (ecommerce Directive), since this Directive no longer appears adequate for governing today's platforms which operate globally, are predominantly managed by algorithms, and host that may be harmful.
- The **adoption of the DSA is a significant achievement resulting from a long-term effort by European authorities to promote responsible moderation practices among major social media platforms**. Over the past two decades, as social networks have expanded, platform operators have increasingly relied on algorithms to curate and moderate content.
- However, the trend towards the privatization and automation of online speech control has raised concerns.

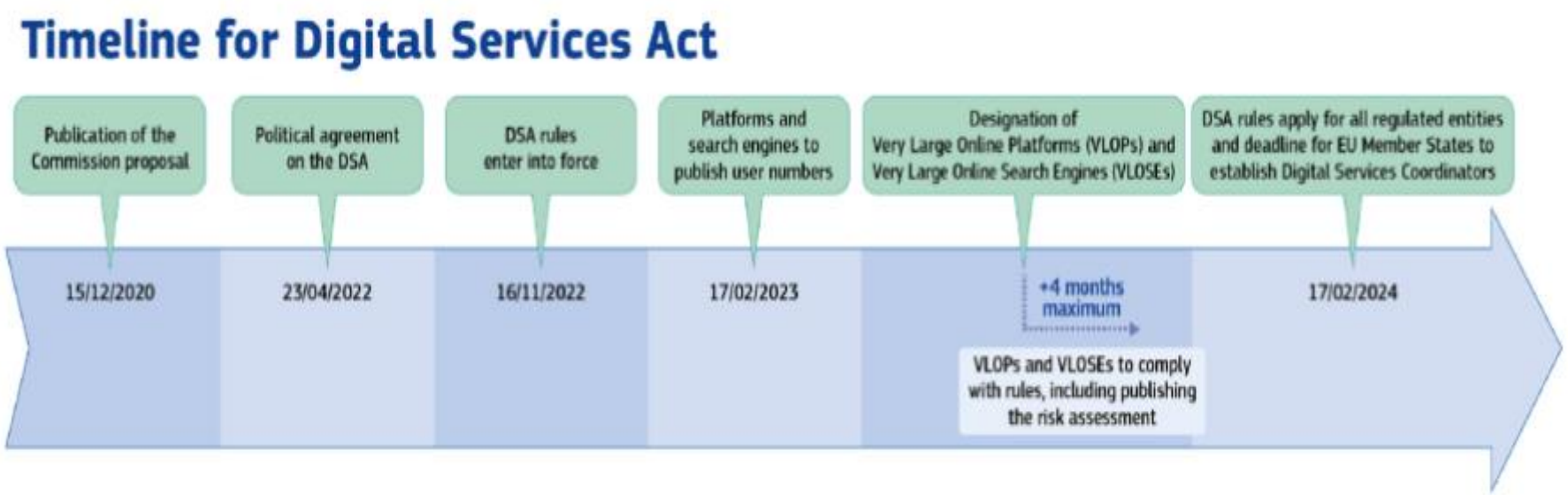
Competition vs. Regulation
The Digital Service Act Package: the case of the DSA

- Flawed moderation practices have prompted European authorities to take action and encourage platforms to implement effective policies against online hate and disinformation.
- In May 2016, Facebook, Microsoft, Twitter, and YouTube entered into an agreement with the EU Commission known as the **"Code of Conduct on countering illegal hate speech online"** to prevent and combat the spread of hate speech on their respective platforms. Over time, other tech companies have also joined this code of conduct.
- In 2018, the EU Commission introduced the aforementioned **"Code of Practice on Disinformation"**, which around 38 tech companies have committed to following. This code was amended and strengthened in 2022 and includes a series of commitments and specific measures designed to address concerns related to disinformation.
- Finally, on March 1, 2018, **the EU Commission published its "Recommendation C/2018/1177 on Measures to Effectively Tackle Illegal Content Online",** which encouraged tech companies to enhance their notice and action procedures, among other things, to more effectively address illegal content on their platforms.

Competition vs. Regulation
The Digital Service Act Package: the case of the DSA

- However, the DSA is not the only recent legislative instrument affecting platforms' liability and content moderation policies.
- Two legislations, in particular, have consistently strengthened the liability of online platforms and increased their obligations.
- **The Directive 2019/790 on copyright and related rights in the Digital Single Market** establishes that providers of online content-sharing services are directly responsible when users illegally upload protected content.
- Providers may be exempt from liability if they have made best efforts to obtain an authorization from the right holder and to block unauthorized content, if they acted expeditiously to remove a content following a notification from a right holder and if they proactively prevented future upload of that content.
- **Regulation 2021/784 of 29 April 2021 on combating terrorist content online** requires hosting service providers to take measures to prevent its dissemination, including removing terrorist content within one hour after receiving a notice from law enforcement. The adoption of the DSA is another evolution in the EU's ongoing efforts to regulate online platforms and fight against illegal activities on the Internet.

Competition vs. Regulation
The Digital Service Act Package: the case of the DSA



Competition vs. Regulation
The Digital Service Act Package: the case of the DSA

European Commission – Press release

Digital Services Act: Commission designates first set of Very Large Online Platforms and Search Engines

Brussels, 25 April 2023

Today, the Commission adopted the first designation decisions under the Digital Services Act (DSA), designating **17 Very Large Online Platforms** (VLOPs) and **2 Very Large Online Search Engines** (VLOSEs) that reach at least 45 million monthly active users. These are:

Very Large Online Platforms:

- Alibaba AliExpress
- Amazon Store
- Apple AppStore
- Booking.com
- Facebook
- Google Play
- Google Maps
- Google Shopping
- Instagram
- LinkedIn
- Pinterest
- Snapchat
- TikTok
- Twitter
- Wikipedia
- YouTube
- Zalando

Very Large Online Search Engines:

- Bing
- Google Search

The platforms have been designated based on the user data that they had to publish by 17 February 2023.

Competition vs. Regulation
The Digital Service Act Package: the case of the DSA

REUTERS® World Business Markets Sustainability Legal Breakingviews Technology Investigations

Retail & Consumer

Zalando sues EU Commission over online content rules, seen as first challenge

By **Foo Yun Chee**

June 27, 2023 10:17 PM GMT+2 · Updated 5 months ago

The logo of fashion retailer Zalando is pictured at the new headquarters in Berlin, Germany, April 10, 2019. REUTERS/Hannibal Hanschke

Competition vs. Regulation
The Digital Service Act Package: the case of the DSA

- Upon assessment of the information obtained during its monitoring, or from reliable sources, the Commission may have the suspicion of infringement. In that case, the Commission may decide to open an investigation and deploy its investigatory tools, such as issuing a request for information, the taking of interviews and inspections of premises.

- At any point in time during the investigation, the Commission can exercise its investigative powers to collect a reliable and consistent body of evidence on the VLOP/VLOSE's compliance.

- In October 2023, the Commission opened the very first DSA compliance investigation by sending requests for information to certain VLOPs.

Competition vs. Regulation
The Digital Service Act Package: the case of the DSA

- The following constitutes an overview of investigatory steps taken by the Commission under the DSA since 25 August 2023 in respect of specific VLOPs and VLOSEs. The taking of such steps should not be taken to imply that the providers of the services listed below have infringed the DSA.

Type of action	Platform	Date of the action	Further information
Request for information	X	12 October 2023	Commission sends request for information to X under Digital Services Act
Request for information	Facebook	19 October 2023	Commission sends request for information to Meta under the Digital Services Act
Request for information	Instagram	19 October 2023	Commission sends request for information to Meta under the Digital Services Act

Competition vs. Regulation
The Digital Service Act Package: the case of the DSA

- The following constitutes an overview of investigatory steps taken by the Commission under the DSA since 25 August 2023 in respect of specific VLOPs and VLOSEs. The taking of such steps should not be taken to imply that the providers of the services listed below have infringed the DSA.

Request for information	TikTok	19 October 2023	Commission sends request for information to TikTok under the Digital Services Act
Request for information	AliExpress	06 November 2023	Commission sends request for information to AliExpress under the Digital Services Act
Request for information	TikTok YouTube	09 November 2023	Commission sends request for information to TikTok and Youtube under the Digital Services Act

Competition vs. Regulation
The Digital Service Act Package: the case of the DSA

- The following constitutes an overview of investigatory steps taken by the Commission under the DSA since 25 August 2023 in respect of specific VLOPs and VLOSEs. The taking of such steps should not be taken to imply that the providers of the services listed below have infringed the DSA.

Request for information	Meta Snap	10 November 2023	Commission sends requests for information to Meta and Snap under the Digital Services Act
Request for information	Amazon	15 November 2023	Commission sends request for information to Amazon under the Digital Services Act

Competition vs. Regulation
The Digital Service Act Package: the case of the DSA

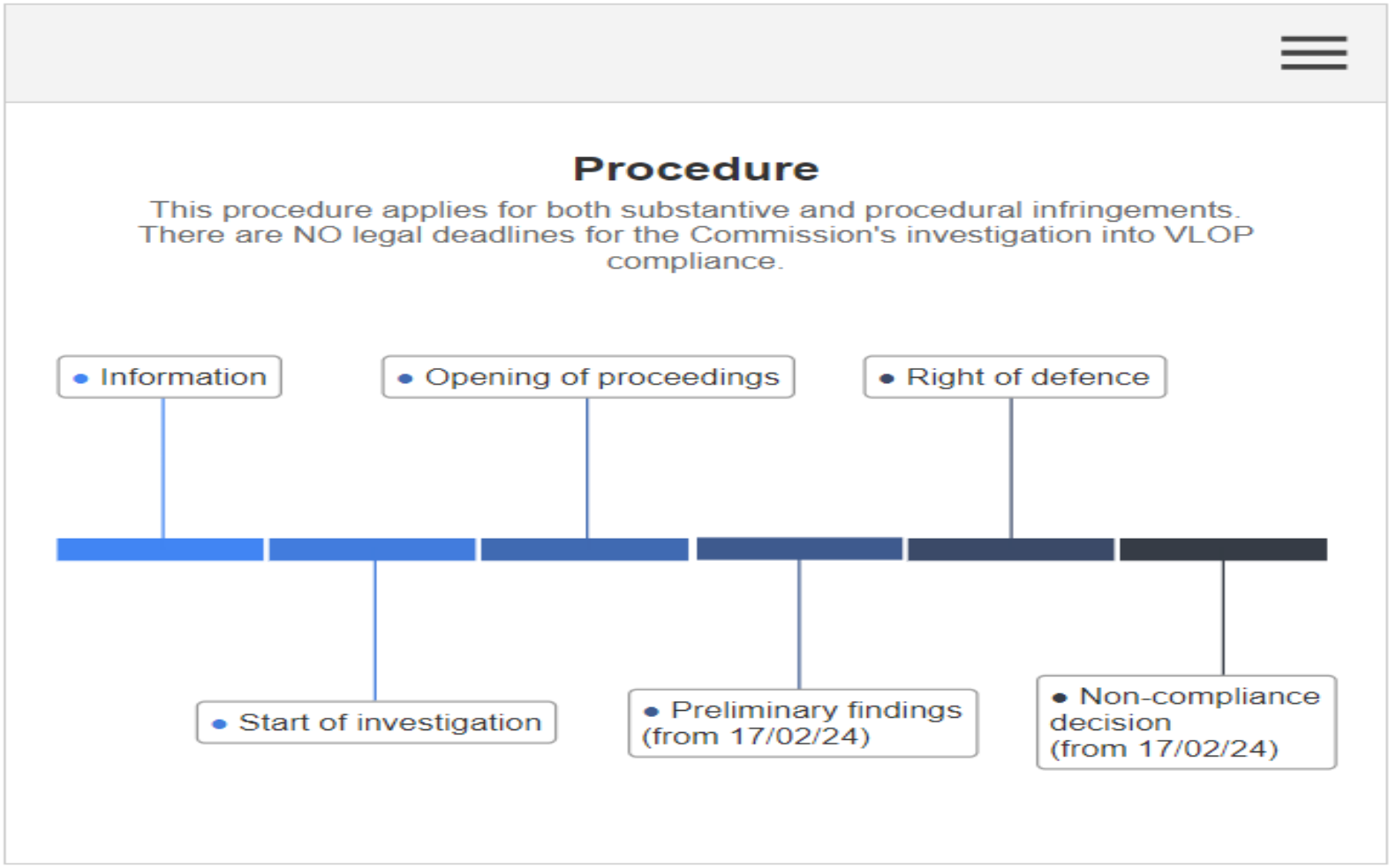
- **Opening of a proceeding**

If the Commission continues to suspect an infringement of the DSA following these investigatory steps, it may open a proceeding. Before adopting a non-compliance decision, a decision imposing fines or a decision imposing periodic penalty payments, the Commission must give the VLOP or VLOSE concerned the opportunity of being heard on its preliminary findings, including any matter to which the Commission has taken objections; and any measures that the Commission may intend to take in view of those preliminary findings.

- **Non-compliance decision**

If the Commission definitely establishes a breach of the DSA, it may adopt a decision imposing fines up to 6% of the global turnover of the VLOP or VLOSE concerned and order that provider to take measures to address the breach by the deadline set by the Commission. That decision may also trigger an enhanced supervision period to ensure compliance with the measures the provider intends to take to remedy the breach. Such a fining decision may be appealed before the EU courts.

Competition vs. Regulation
The Digital Service Act Package: the case of the DSA



Competition vs. Regulation
The Digital Service Act Package: the case of the DSA

- The Digital Services Act has a vast and comprehensive scope that aims to **regulate the activities of "intermediary services" offering digital services** to legal entities in the European Union, as stated in Article 2.

- **It is immaterial whether the provider is based in the EU or not under the DSA**. If the service provider does not have an establishment in the EU, the DSA's applicability is subject to the "substantial connection" condition with the EU, as outlined by Article 3(d). This means that the provider must have a significant number of EU-based users or targets its activities towards a specific EU member state, such as by using a relevant top-level domain name (Article 3(e) DSA).

- All providers of intermediary services must appoint a **single point of contact allowing for direct communication with the competent supervisory authorities and users**, as provided by Article 11 and 13.

Competition vs. Regulation
The Digital Service Act Package: the case of the DSA

- The key features of the Digital Services Act can be summarized in **five points**.
- **First**, it is an asymmetrical regulation.
- **Second**, it upholds the principle of exemption from liability while introducing the Good Samaritan principle.
- **Third**, it introduces new obligations for content moderation to combat undesirable content effectively and better protect users' rights.
- **Fourth**, it includes specific provisions aimed at enhancing user and consumer protection.
- **Finally**, it contains very specific implementation and enforcement procedures.

Competition vs. Regulation
The Digital Service Act Package: the case of the DSA

1. Asymmetric regulation

- While the scope of the Digital Services Act is broad, it solely governs **"intermediary services“** rather than the “**information society services”** regulated by the E-Commerce Directive.
- “Intermediary services” refer **to those that transmit and store user-generated content**, as per Article (3)(g) DSA. The DSA further classifies **different types of "intermediary services"** that are available to users in the European Union.
- The **first three categories** were already present in the E-commerce Directive and **include "mere conduit" services, "caching" services, and "hosting" services**.
- The DSA adds **two new categories**: **"online platforms"**, which are a category of hosting services that disseminate information to the public, and **"online search engines"**.

Competition vs. Regulation
The Digital Service Act Package: the case of the DSA

1. Asymmetric regulation

- The distinctions among different service types are significant because the **DSA is not meant to be uniformly applied to all regulated service providers**. Instead, the **DSA takes the form of a "layer cake"**, **designed to be applied asymmetrically** with rules that vary depending on provider characteristics.
- In other words, the **DSA's obligations are structured as a pyramid**, with layered requirements from the bottom to the top. At the base of the pyramid, **the first layer encompasses all intermediary services that have very basic obligations, followed by hosting services, and then online platforms**.

Competition vs. Regulation
The Digital Service Act Package: the case of the DSA

1. Asymmetric regulation

- Moving up the pyramid reveals increasingly **stringent obligations that apply to fewer and fewer categories of providers**.
- At the top of the pyramid, **the most extensive and restrictive obligations are imposed on very large online platforms (VLOPs) or search engines (VLOSEs)** that have at least 45 million average monthly active users in the EU. These additional obligations are justified by the **systemic risks** they pose due to their size.

Competition vs. Regulation
The Digital Service Act Package: the case of the DSA

1. Asymmetric regulation

- While large companies face heavier obligations, **micro and small companies are exempt from certain obligations**. For instance, transparency obligations (article 15), provisions applicable to online platforms (section 3) and provisions applicable to platforms allowing consumers to conclude distance contracts with traders (section 4) are not applicable to micro or small enterprises.
- These small enterprises are defined as companies with **fewer than 250 employees and an annual turnover under €50 million or an annual balance sheet total under €43 million**, as per Recommendation 2003/361/EC.
- Despite this exemption, it could be argued that the threshold are too low and that the DSA's stringent obligations may negatively impact the financial stability and growth of small and medium-sized enterprises, since the companies that are just above these thresholds would be penalized.
- As a result, the DSA would benefit larger platforms and search engines that have the resources to comply with its provisions. In any case, an assessment of the DSA's impact on micro and small companies will be conducted by the Commission after five years, as provided by Article 91(2)(d).

Competition vs. Regulation
The Digital Service Act Package: the case of the DSA

2. Liability exemption

- **The DSA preserves the exemption from liability established by the E-Commerce Directive in 2000**, with additional clarifications. One significant addition is the inclusion of the **Good Samaritan clause**, which draws inspiration from section 230 of the US Communications Act of 1934.
- The E-Commerce Directive introduced a **new category of service providers called "hosting service providers"** and provided, in its article 14, that these hosting providers are exempt from liability for content stored at a user's request if **they have no actual knowledge of its illegality**. Providers of mere conduit and caching services are similarly not held liable for the information they transmit or store for their users.
- The DSA upholds the liability exemption provided by the E-Commerce Directive for over 20 years. **Article 6 of the DSA provides hosting providers with protection from liability for illegal content stored on their platforms**.

Competition vs. Regulation
The Digital Service Act Package: the case of the DSA

2. Liability exemption

- This protection applies **if they act "expeditiously" to remove access to the content once they become aware of its illegality**. Similarly, Article 4 specifies that mere conduit service providers are not liable for the information transmitted or accessed if they do not initiate the transmission, select the receiver of the transmission or modify the information contained in the transmission.
- Under Article 5, caching service providers are not liable if they do not modify the information and act expeditiously to remove or to disable access to the information upon obtaining actual knowledge of the fact that the information has been removed from its initial source or when required by law or a court order. They must also not interfere with the lawful use of technology.
- Unlike the provisions of the E-Commerce Directive, which had to be transposed into national law, **this liability exemption now applies directly and uniformly across all EU countries**.

Competition vs. Regulation
The Digital Service Act Package: the case of the DSA

2. Liability exemption

- **Article 7 of the DSA allows providers to carry out voluntary investigations or take other measures to detect, identify and remove illegal content**. However, some may worry that this could lead to platforms being considered playing an active role that gives them knowledge or control over the content and losing their exemption from liability as a result. In reality, **engaging in these investigations does not automatically make platforms responsible for the content**. **The Good Samaritan clause was added to the DSA in response to requests from online platforms** for greater clarity and reassurance that they could take voluntary steps to remove illegal content without losing their liability exemption.
- The newly introduced Good Samaritan clause draws inspiration from Section 230 of the US Communications Act of 1934, specifically 230(c)(2)(A), which offers Good Samaritan immunity to platforms. **This immunity allows platforms to intervene in good faith on content without incurring any liability**.
- In the virtual space, **the Good Samaritan immunity guarantees that providers and users of online services will not be held liable for any action taken in good faith to remove or restrict access to content that the provider or user considers objectionable**. Under the DSA, the Good Samaritan clause ensures that providers **can detect and remove illegal content without losing their liability exemption**.

Competition vs. Regulation
The Digital Service Act Package: the case of the DSA

3. New due diligence obligations for content moderation

- **The DSA introduces additional obligations for intermediary service providers beyond the existing knowledge-based liability principle that has been in place for over two decades**. The new obligations provided by the DSA stem from concerns about the effectiveness of the existing knowledge-based liability principle in compelling platforms to address illegal content.
- **The DSA's new obligations are primarily centered around the content moderation activities carried out by the platforms**. This is why the DSA introduces, in Article 3(t), a **broad definition of "content moderation"** as "the activities, whether automated or not, undertaken by providers of intermediary services, that are aimed, in particular, at detecting, identifying and addressing illegal content or information incompatible" with the providers' terms and conditions, including "measures taken that affect the availability, visibility, and accessibility of that illegal content or that information, such as demotion, demonetisation, disabling of access to, or removal", or that affect the ability of users to publish or transmit information, such as the termination or suspension of a user's account.

Competition vs. Regulation
The Digital Service Act Package: the case of the DSA

3. New due diligence obligations for content moderation

- With this definition, **the DSA recognizes the crucial role played by platforms in moderating content**, often using automated tools. It also acknowledges that this moderation activity is not only based on the applicable laws, but **also governed by the platforms' terms and conditions**, which is reflected by the fact that most major platforms now publish increasingly detailed content policies.
- Consequently, the DSA's new obligations related to content moderation can be grouped into **four categories**: **combating illegal content, upholding procedural safeguards in moderation, ensuring transparency, and managing systemic risks**.

3. Combating illegal content

- The DSA not only maintains the liability exemption, but it also imposes **new obligations on online platforms to effectively combat illegal content**. This fight against illegal content involves the users and relies mainly on user notifications. The DSA includes extensive guidelines on how to handle user notifications, which have not been as detailed in the past. **Article 16 requires providers of hosting services to establish accessible "notice and action" mechanisms that allow anyone to notify them of the presence of illegal content**.
- The main goal is to make sure that these notice and action procedures are effective in combating illegal content while also safeguarding the rights of users, including protection against unjustified removal.

Competition vs. Regulation
The Digital Service Act Package: the case of the DSA

3. Combating illegal content

- Therefore**, hosting platforms must implement efficient reporting mechanisms and have clear and user-friendly reporting systems in place to enable users to report illegal content**.
- To that end, providers are required by **Article 12 to designate a single point of contact to facilitate direct and rapid communication through electronic means**.
- In addition, Article 22 requires providers to **prioritize reports from trusted flaggers**, which are entities designated by competent national authorities that have demonstrated expertise and competence in identifying illegal content.
- Hosting service providers must **process received notifications in a timely, diligent, non arbitrary, and objective manner, as provided by Article 16(6)**.
- However, it must also be highlighted that providers do not have to take action on the reported content following the reception of a user's notice. **They are only expected to remove the content if the notice is sufficiently clear and adequately substantiated, and if the illegality can be established without a detailed legal examination, as outlined by Article 16(3).**

Competition vs. Regulation
The Digital Service Act Package: the case of the DSA

3. Combating illegal content

- The fight against illegal content also depends on **effective collaboration with national authorities**.
- **Article 18 imposes an obligation on online platforms to cooperate with national law enforcement or judicial authorities and promptly notify them of any content that may give rise to suspicions of criminal offenses posing a threat to the life or security of individuals**.
- The purpose of this obligation is to **prevent or swiftly address serious crimes**. However, this obligation is limited to criminal offenses that pose a threat to the life or safety of one or more persons, and it does not cover other criminal acts. Additionally, providers must comply with any instructions from authorities to act against illegal content and must justify the measures taken.
- **Articles 9 and 10 provide that national judicial or administrative authorities may issue orders requiring providers to act against specific illegal content or provide information about certain users, but such orders must not constitute a general monitoring obligation**.
- Indeed, the **DSA maintains, in Article 8, the prohibition of mandated general monitoring that already existed in the E-Commerce Directive**. The prohibition concerns obligations "of a general nature" as opposed to obligations "in a specific case", as stated by Recital 30. An example of an obligation “of a general nature” is **the obligation to introduce a system for filtering all electronic communications for an unlimited period and at the provider’s expense in order to block unlawful use or transfer of copyrighted works**. However, an obligation for a service provider to identify and remove specific information deemed illegal by a court and equivalent information is not covered by the prohibition. Despite existing precedents, it is not always easy to distinguish between general and specific obligations.

Competition vs. Regulation
The Digital Service Act Package: the case of the DSA

3. Upholding procedural safeguard in content moderation

Online platform providers not only moderate content in accordance with the relevant laws and regulations, but also **set their terms and conditions, which allow them to determine their own content policies and decide what content to host or remove**.

These moderation standards serve as a private norm that governs online speech in practice. The **DSA is actually one of the first pieces of legislation to recognize the crucial role played by terms and conditions in content moderation**, while also trying to guarantee that the determination of these standards and their enforcement is in accordance with the fundamental rights of users.

To that end, **the DSA adopts a procedural perspective and imposes due process obligations** intended to serve as safeguards against possible arbitrariness by platforms. Furthermore, the DSA does not interfere with the freedom of hosting providers to establish their own content policies.

Competition vs. Regulation
The Digital Service Act Package: the case of the DSA

3. Upholding procedural safeguard in content moderation

The DSA stipulates in **article 14 that providers are required to clarify "any restrictions that they impose in relation to the use of their service" in their terms and conditions**.

The information provided must include «any policies, procedures, measures and tools used for the purpose of content moderation, including algorithmic decision-making, and human review as well as rules of procedure of their internal complaint handling system».

This requirement has been **analyzed as a form of "codification" of moderation rules**, enabling the enforcement of "the rule of law's principles of legality, predictability, and accessibility for the imposition of sanctions".

Furthermore, **Article 14(4) mandates that service providers must act diligently, objectively, and proportionately while applying and enforcing their terms and conditions**, taking into account the rights and legitimate interests of all parties involved, including users' fundamental rights.

Competition vs. Regulation
The Digital Service Act Package: the case of the DSA

3. Upholding procedural safeguard in content moderation

In addition to clarifying their terms of use, **platforms are obliged to provide a clear and specific explanation of the reasons for the decisions they make about content provided by users constituting either illegal content or being incompatible with their terms and conditions**.

This “statement of reasons” will allow users to challenge the moderation decisions made about them.

The scope of this obligation to provide explanation is particularly broad. Indeed, as illustrated by the wording of the abovementioned Article 3(t), the DSA's definition of moderation actions is comprehensive and all-encompassing.

Article 17 stipulates an **explanation must be provided in the case of “any restrictions of the visibility”**, including “removal of content, disabling access to content, or demoting content”, and in case of suspension, termination or other restriction of monetary payments, of the service, or of the service’s account. In other words, the statement of reasons is required in cases where content is removed, demonetize or demoted, including instances of "shadow banning," where a user's content is concealed from others without their knowledge.

Competition vs. Regulation
The Digital Service Act Package: the case of the DSA

3. Upholding procedural safeguard in content moderation

According to Article 20, providers must establish an efficient internal complaint handling system that allows users to challenge moderation decisions they believe to be unjust or incorrect.

This system should enable users to contest decisions related to the removal of allegedly illegal content or the suspension of their account or service provision, as well as decisions not to act on a notice of illegal content. Moderation decisions must be reversed when the complaint contains sufficient grounds.

The DSA provides that **such complaints must be reviewed "in a timely, non-discriminatory, diligent and non-arbitrary manner"**, as stated by Article 20(4).

According to Article 20(6), the appeal decisions must be "taken under the supervision of appropriately qualified staff, and not solely on the basis of automated means".

Competition vs. Regulation
The Digital Service Act Package: the case of the DSA

3. Upholding procedural safeguard in content moderation

- Users also have **the option to submit disputes to an out-of-court dispute settlement body certified in one of the Member States** based on their independence and expertise, as per Article 21.
- However, this provision may not be effective since Article 21(3) subparagraph 3 provides that “the certified out-of-court dispute settlement body shall not have the power to impose a binding settlement of the dispute on the parties”.
- This means that in case of persistent disagreement on moderation decisions, **users will have no other option than to go to court at their own expense, as provided by Article 21(1), subparagraph 3**. Indeed, Article 54 provides that users can always request compensation for any damages or losses incurred due to a breach of the DSA. They can even bring representative actions for the protection of collective consumer interests, as per Article 90.
- **Article 23 provides that online platform providers are required to suspend services to such users, subject to several safeguards**. The user must have been previously warned and the suspension must also be limited to a reasonable period of time. Providers must assess each case individually, in a timely, diligent, and objective manner, and clarify their policies in advance in the terms and conditions.

Competition vs. Regulation
The Digital Service Act Package: the case of the DSA

3. Ensuring transparency

- The DSA not only implements procedural due process but also seeks to **incentivize platforms to act in a responsible manner by imposing precise transparency obligations on them**, especially regarding their moderation practices.
- According to Article 15 of the DSA, **all intermediaries except micro and small enterprises must report annually on their content moderation**. The report must provide information about content moderation at the providers' own initiative, including the use of automated tools. It must include, among other things, the number and type of measures taken that affect information availability, visibility and accessibility and the number of orders received from Member States' authorities categorized by the type of illegal content concerned. Hosting providers must also disclose "the number of notices submitted categorized by the type of alleged illegal content concerned, the number of notices submitted by trusted flaggers, any action taken pursuant to the notices by differentiating whether the action was taken on the basis of the law or the terms and conditions of the provider, the number of notices processed by using automated means and the median time needed for taking the action" (Article 15(1)(b)).

Competition vs. Regulation
The Digital Service Act Package: the case of the DSA

3. Ensuring transparency

- Online platforms must add information about the basis for the complaints received, the decisions taken following those complaints, the median time needed for taking those decisions and the number of instances where those decisions were reversed. They must also provide information about the number of disputes submitted to out-of-court settlement bodies and the number of service suspensions following the publication of manifestly illegal content or manifestly unfounded notices or complaints, as provided by Article 24. The information reported must be categorized by the type of illegal content or violation of the terms and conditions of the service provider, by the detection method and by the type of restriction applied.
- The DSA imposes increased transparency and accountability measures for very large online platforms (VLOPs) and search engines (VLOSEs). These operators must publish transparency reports twice a year that include information about their content moderation resources and the qualifications of their moderators, as provided by Article 42. In addition, VLOPs and VLOSEs must provide regulators with access the data needed to verify that they are in compliance with the DSA, as stated by Article 40(1)). In this respect, they must be able to explain to regulators the design, logic, operation and testing of their algorithmic systems, including their recommendation systems.

Competition vs. Regulation
The Digital Service Act Package: the case of the DSA

3. Managing systemic risks

- **Article 34 of the DSA stipulates that very large online platforms (VLOPs) and search engines (VLOSEs) with at least 45 million users must evaluate and address "systemic risks" through appropriate policies**.
- They must analyze the extent to which their moderation, recommendation, and advertising systems may affect those systemic risks. This should be done annually and also prior to the deployment of functionalities that are likely to have a critical impact on the risks identified.
- Systemic risks pertain to issues such as illegal content, hate speech, privacy violations, election manipulation, and other similar problems. Moreover, content that generates adverse effects on fundamental rights, civic discourse, electoral processes, public security, gender-based violence, public health, minors, and personal well-being may also lead to systemic risks.
- Although Article 35(1) mentions "illegal hate speech or cyber violence", the definition of systemic risks encompasses content that is not necessarily illegal but may cause problems, such as misinformation on public health, climate change, or politics.
- After assessing systemic risks, VLOPs and VLOSEs should implement "reasonable, proportionate, and effective mitigation measures" to counter such risks, as provided by Article 35.

Competition vs. Regulation
The Digital Service Act Package: the case of the DSA

3. Managing systemic risks

- Moreover, the DSA introduces a unique monitoring system to enforce compliance with these obligations, which includes vetted researchers in addition to national and European regulatory bodies.
- First, VLOPs and VLOSEs are required to provide their assessments of systemic risks to the European Commission and relevant Digital Services Coordinators upon request, as per Article 35(2). The European Board of Digital Services will work with the Commission to publish annual reports on the identification and assessment of systemic risks, including best practices for mitigating these risks (Article 35(2)). Additionally, the Commission may issue guidelines and recommend actions in cooperation with Digital Services Coordinators (Article 35(3)). Within this framework, regulators play a role in determining and approving the strategies implemented to mitigate systemic risks.
- Second, regulators will also benefit from the expertise of researchers who will be provided with access to platform data to evaluate systemic risks. Indeed, Article 40 states that VLOPs and VLOSEs must provide internal data on request to researchers vetted by national regulators. This provision allows researchers to request whatever data they need to asses those risks and to go much further than the analyses provided in the reports prepared by the platforms themselves.

Competition vs. Regulation
The Digital Service Act Package: the case of the DSA

3. Managing systemic risks

- By providing for measures to address the "systemic risks" generated by the operation of large platforms and search engines, the DSA goes far beyond the simple fight against content deemed illegal by the national laws of the various Member States. This includes considering not only illegal content but also "lawful but awful" content that may be harmful. In particular, while European national laws often criminalize hate speech, the same cannot be said of disinformation, which is often difficult to define or demonstrate, and is rarely sanctioned as such.
- In this context, the category of systemic risks can ideally serve as a basis for implementing effective policies to fight disinformation, in line with the Code of Practice on Disinformation implemented at the European Union level. Furthermore, Article 35 enables regulators to issue guidelines and recommendations to mitigate systemic risks, which could include suggestions on the content of platforms' terms and conditions and content policies.

Competition vs. Regulation
The Digital Service Act Package: the case of the DSA

4. Other obligations

- In addition to regulating moderation practices, the DSA contains provisions designed to protect users of online services more generally and in particular consumers who use the services of marketplaces and collaborative economy platforms.
- The DSA includes specific provisions for recommendation systems. According to Article 27, online platforms must provide precise and intelligible information in their terms and conditions about the main parameters used by their recommendation systems.
- Furthermore, the DSA strictly regulates online advertising. Advertising platforms must fully disclose their practices and targeting methods to advertisement recipients as per Article 26.
- Online platform providers must indicate on whose behalf and why the advertisement is being displayed to the user (Art. 26(1) DSA). VLOPs and VLOSEs must maintain a publicly accessible repository containing information about advertisements presented, including their content and the companies on whose behalf they were made, as provided by Article 39 DSA.
- Additionally, article 26(3) prohibits displaying advertising based on profiling using sensitive data such as political opinions, religious beliefs, and sexual orientation. Targeted advertising of minors based on their personal data is prohibited, and specific protection measures must be put in place to ensure their safety online, as per Article 28.

Competition vs. Regulation
The Digital Service Act Package: the case of the DSA

4. Other obligations

- Finally, the DSA strictly prohibits the use of "dark patterns" that manipulate internet users into performing a specific action, such as subscribing to a service, by subconsciously influencing them. According to Article 25(1), providers of online platforms cannot “design, organize or operate their online interfaces in a way that deceives or manipulates” users or in a way that “otherwise materially distorts or impairs the ability of” users “to make free and informed decisions”.

Competition vs. Regulation
The Digital Service Act Package: the case of the DSA

4. Specific protection of consumers on marketplaces and collaborative economy platforms

- Online platforms that allow the conclusion of distance contracts between consumers and traders, such as marketplaces and collaborative economy platforms, have specific obligations that they must fulfill. These obligations include obtaining certain information about their professional users, such as their name, contact details, and identification and registration information, through "know your customer" protocols.
- Article 30 provides that online platforms must make best efforts to verify the accuracy and completeness of the information provided by professional users.
- In addition, these platforms are required by Article 31 to ensure that their interface is designed in a way that complies with consumer law regarding pre-contractual information obligations and product safety.

Competition vs. Regulation
The Digital Service Act Package: the case of the DSA

4. Specific protection of consumers on marketplaces and collaborative economy platforms

- Additionally, these platforms are required to make “reasonable efforts to randomly check in any official, freely accessible and machine-readable online database or online interface whether the products or services offered have been identified as illegal”, as per Article 31 (3).
- If they become aware of any such illegality, they must inform the consumers who purchased the illegal product or service about the trader's identity and all relevant means of redress, as provided by Article 32 DSA.

Competition vs. Regulation
The Digital Service Act Package: the case of the DSA

5. Implementation of the DSA

- In certain respects, the implementation of the DSA is less complicated than that of the Ecommerce Directive, as the Regulation is directly applicable and does not require a transposition law to be adopted by each Member State. However, implementing the DSA requires to determine which authorities are competent to enforce it and which measures these authorities can take.

Competition vs. Regulation
The Digital Service Act Package: the case of the DSA

5. Implementation of the DSA

- The competent authorities to control the implementation of the DSA are the national authorities.
- Member States will designate "National Coordinators of Digital Services", as per Article 49. These coordinators will receive complaints from users, have investigative powers, and may impose sanctions. They will also convene in a European Board for Digital Services, an advisory body designed to promote coordination and cooperation between them.
- The DSA establishes that the Member State in which an intermediary service provider is established has exclusive jurisdiction over that provider, as stated by article 56(1). This principle aligns with the country of-origin rule established in Article 3 of the E-Commerce Directive. Recital 123 of the DSA defines "main establishment" as the location of a provider's head or registered office, where the primary financial functions and operational control take place.
- However, it may be difficult to determine exactly which authorities are responsible for enforcing the DSA. For VLOPs and VLOSEs, the European Commission has the power to enforce the DSA in collaboration with national authorities and coordinators. The Commission holds exclusive authority over obligations that apply solely to VLOPs and VLOSEs, as outlined in Article 56(2) of the DSA. Both National Coordinators and the Commission have jurisdiction over all other DSA obligations for VLOPs and VLOSEs, as per Article 56(3). The Commission will work with national coordinators to investigate potential violations and determine whether to impose fines.

Competition vs. Regulation
The Digital Service Act Package: the case of the DSA

5. Implementation of the DSA: enforcement

The potential severity of penalties for non-compliance with the DSA should incentivize

companies to comply with its provisions. Penalties will be defined in national law and must be “effective, proportionate, and dissuasive”, as provided by Article 52. The maximum penalty cannot exceed 6% of the company’s annual turnover. For some infringements, such as providing incorrect or incomplete information or refusing to comply with inspections, the maximum penalty may be raised to 1% of annual turnover. Companies may also face periodic fines, with each monthly payment not exceeding 5% of their daily turnover.

The European Commission can also impose fines up to these amounts. Repeated non-compliance may result in access restrictions but not a definitive ban within the EU. Under article 82 of the DSA, the European Commission can request a regulator to ask a judicial authority to temporarily restrict user access if there is a serious and persistent breach causing significant harm and involving a criminal offense threatening people’s safety or lives. Therefore, non-compliance may result in temporary access restrictions and fines at worst.

Competition vs. Regulation
The Digital Service Act Package: the case of the DSA

5. Implementation of the DSA: enforcement

In addition to potentially high penalties for non-compliance, the DSA includes mechanisms designed to encourage compliance by the largest entities.

VLOPs and VLOSEs must appoint a compliance officer, as per Article 41. VLOPs and VLOSEs must also conduct annual independent audits to assess their compliance with the DSA and submit reports to competent authorities (article 37). These reports must include information on measures taken to prevent the dissemination of illegal content on the platform, as well as details of the platform's internal complaint handling system and content moderation procedures.

Compliance with the provisions for controlling systemic risks by VLOPs and VLOSEs is based on an "enhanced supervision system" provided by Article 75. Under this system, the Commission may request that very large platforms provide regulators with an action plan to address potential violations of the DSA.

This action plan may include conducting an independent audit. The Commission has the discretion to determine whether the action plan is sufficient and may reject it if deemed inadequate.

Finally, the DSA stipulates in Article 45 that regulators must encourage and facilitate the development of voluntary codes of conduct at the Union level to support the proper application and ensure consistent implementation of the Regulation, particularly in regards to combating illegal content and mitigating systemic risks.

The Commission and the European Board of Digital Services are tasked with promoting and supporting the creation of these codes of conduct.

Università Europea di Roma

Co-funded by the Erasmus+ Programme of the European Union

COMPETITION VS. REGULATION IN DIGITAL MARKETS

THE DIGITAL SERVICES ACT PACKAGE: THE CASE OF THE DIGITAL GOVERNANCE ACT («DGA»)

Competition vs. Regulation: the case of the DGA

- The Data Governance Act (“DGA”) is a cross-sectoral instrument that aims to make more data available by regulating the re-use of publicly/held, protected data, by boosting data sharing through the regulation of novel data intermediaries and by encouraging the sharing of data for altruistic purposes. Both personal and non-personal data are in scope of the DGA, and wherever personal data is concerned, the General Data Protection Regulation (GDPR) applies. In addition to the GDPR, inbuilt safeguards will increase trust in data sharing and re-use, a prerequisite to making more data available on the market.

Competition vs. Regulation: the case of the DGA

- Chapter II of the Act aims to **unlock more value in data held by the public sector**, by opening up this data for **re-use.** Recital 5 explains the objective well:
- "The idea that data that has been generated or collected by public sector bodies or other entities at the expense of public budgets should benefit society has been part of Union policy for a long time [via the Open Data Directive] … However, **certain categories of data (commercially confidential data, data subject to statistical confidentiality, data protected by intellectual property rights of third parties, including trade secrets and personal data) in public databases is often not made available**… not even for research or innovative activities in the public interest…".
- Chapter II aims to promote use of these "difficult" types of data. The provisions **apply to public sector bodies and aim to facilitate "re-use" of the data** – that is, use for commercial, or non-commercial purposes, other than the initial public task for which the data were produced. There are exclusions – for example, the **Act does not cover data held by public undertakings** (owned by public bodies), broadcasters, cultural establishments, data which are protected for reasons of national security, defence or public security.

Competition vs. Regulation: the case of the DGA

- Like the Open Data Directive, **the Act does not oblige public sector bodies to allow re-use of data, but where data are made available for re-use then it requires that access arrangements must be non-discriminatory, transparent, proportionate, objective and may not restrict competition**. Exclusive access arrangements are restricted. There are also restrictions on fees payable for access.
- Public sector bodies who do provide access must ensure that they **preserve the protected nature of the data**. By way of example, this could mean only releasing data in anonymous form. Or it could mean using secure processing environments – physical or virtual environments which allow access to data, whilst ensuring compliance with other laws and preserving the protected nature of the data. Recital 6 specifically calls put the potential for use of differential privacy and synthetic data as ways of allowing exploitation of data. Those who wish to re-use the data, must agree to continue to respect the protected nature of the data; where data has been released that was originally personal, then this would include agreeing not to attempt to re-identify data subjects.

Competition vs. Regulation: the case of the DGA

- If a public sector body receives a request to release data, but cannot do so in a compliant way, even by using the techniques above, then **it has an obligation to use best efforts to seek consent to re-use from the data subject/ affected person**, unless this would involve disproportionate effort.
- Allowing re-use of data which is personal, confidential, or otherwise protected by IPRs, whilst simultaneously not prejudicing those same interests, will be difficult. To assist in this, the Commission requires **each Member State to have a competent body to support public authorities in these tasks**. To facilitate re-users of the data, the Member State must also ensure that there is a single point, to which requests for re-use can be directed. This must also list all datasets available for re-use. The Commission will also create an EU wide single access point.

Competition vs. Regulation: the case of the DGA

- Chapter III of the Act **aims to encourage a new market in neutral data intermediation services**. This is on the basis that, “specialised data intermediation services that are independent from data subjects and data holders [person with a right to license data], and from data users [person with a right to use data], could have a facilitating role in the emergence of new data-driven ecosystems…”. The Chapter seeks to achieve this by imposing a **licensing regime on data intermediation services**, where the licence conditions are designed to ensure independence.
- Data intermediation services are services which **aim to establish commercial relationships, for the purpose of data sharing, between an indeterminate number of data holders (or data subjects) and data users**. These commercial relationships could be established through technical, legal or other means. The concept is limited to pure facilitation of data sharing – accordingly, providers who enrich data or otherwise add value to it are not included. Providers who intermediate copyright protected content; closed group arrangements; and arrangements by a single data holder to allow exploitation of its own data are all excluded, as are intermediation services provided by public sector bodies without “aiming to establish commercial relationships for purpose of data sharing”. Browsers and email service providers and account information service providers under the PSD2 Directive are also excluded. However, data marketplaces are specifically mentioned as a type of intermediation service.

Competition vs. Regulation: the case of the DGA

- Intermediation services could also include services set up to intermediate between data subjects who want to make their personal data available, and data users who want to use such personal data. Here, the Act notes the risk of “misaligned incentives”. Any intermediation service provider offering services to data subjects must “act in their best interests” when facilitating the exercise of their rights, in particular in providing information about the intended uses of data (and any uses of consented data outside the EU). The Act also anticipates the creation of specialised forms of data intermediaries, “data co-operatives”, which are – in effect – owned by the data subjects they represent and whose principal objective is to support data subjects in exercising their rights.

- The Act sets up a two-tier licensing structure. All intermediation service providers must notify (i.e. complete a filing with) the relevant competent authority and must meet specified conditions. Intermediation service providers may also (but are not required to) ask the competent authority to confirm if the provider meets these conditions. If the competent authority issues this confirmation, the provider is then able to use a to-be-developed Commission logo and to use the legend “provider of data intermediation services recognised in the Union” in communications. The competent authority for a service provider is the authority in the member state where the service provider has its main establishment and service providers with no EU presence must appoint a legal representative in the EU – all concepts familiar from the GDPR.

Competition vs. Regulation: the case of the DGA

- Those offering intermediation services must meet conditions set out in Art.11, all designed to ensure independence. These conditions include the following: intermediation services have to be offered by a separate legal person (i.e. not offering other services); separate use of the data is prohibited; pricing cannot be linked to take up of other services; metadata about service use cannot be used for other purposes (but prevention of fraud/ cyber risk and service development is acceptable); data must be provided in the format received; it can only be converted if this is to enhance interoperability and the provider must allow an opt-out from this; the provider can offer tools to facilitate exchange of data – but must have approval of the data holder/ data subject to do this; licences must be on FRAND type terms; the provider must ensure availability and interoperability with other intermediation services; must put in place technical, organisational and legal measures to prevent transfer or access to non-personal data that would be unlawful & must notify the data holder of any unauthorised access/ use of non-personal data that has been shared and appropriate security measures must be maintained (in other words, GDPR style protections are introduced for non-personal data which is shared via an intermediation service) and, lastly, logs of all intermediation activity must be maintained.
- The recitals to the Act give the impression that data intermediation services will be new types of services, tied to yet-to-exist developments in the data economy. However, it seems possible that many existing organisations may be offering data intermediation services. The provisions seem to be particularly applicable in the ad-tech space. For example:

- Those offering data marketplaces; and
- (possibly) consent management platforms

could well be in-scope.

- Organisations offering services which facilitate access to personal data should, therefore, review the provisions in Chapter III carefully. If in scope, they have 24 months from the date the Act becomes applicable to meet the requirements in the Act.

Competition vs. Regulation: the case of the DGA

Data altruism

The Act defines "data altruism" as "the consent by data subjects to process personal data pertaining to them, or permissions of other data holders **to allow the use of their non-personal data without seeking a reward that goes beyond a compensation related to the costs they incur making their data available, for purposes of general interest**, …, such as healthcare, combating climate change, improving mobility, facilitating the establishment of official statistics, improving public services, public policy making or scientific research purposes in the general interest".

The provisions in the Act on data altruism are relatively light touch. The Act notes that Member States may wish to promote altruism (including by allowing individuals to make personal data held by public sector bodies more widely available), but **there is no obligation to do so**. Likewise, the Act sets out a registration scheme for data altruism organisations, but – unlikely data intermediaries – **registration is voluntary**. Member States must designate a competent authority to manage the registration process and, as with data intermediaries, there are arrangements for organisations operating in multiple member states to register via their main establishment and for those with no EU establishment to nominate a representative.

Competition vs. Regulation: the case of the DGA

Data altruism

Under the Act, the lawful basis for altruistic use of a data subject's data **is consent given by the data subject**. The Commission is to **develop an European consent form for the altruistic transfer of data**, in order to **reduce the costs involved in obtaining consent and to facilitate data portability** (when the data to be transferred are not in the possession of the data subject).The form is to be modular, allowing for customisation for sector-specific consent templates. Some sector-specific working groups have already been working along these lines in order to explore this concept of data altruism, e.g. in the area of health and scientific research. Particularly relevant for this purpose is the project "Towards European Health Data Space" which develops European principles for the secondary use of health data and has recently produced a first set of data altruism definitions, use cases and conclusions that can be taken as a reference document when establishing a methodology for carrying out impact assessments aimed at mitigating possible risks that may arise.

Competition vs. Regulation: the case of the DGA

Data altruism

The term altruism seems to imply that **data should be given without expectation of anything in return**, and to suggest that the provisions are of relevance solely to not-for-profit organisations, but this is not necessarily the case. Many public bodies will probably participate in this data exchange without receiving anything in return in the first instance, but with the intention of being rewarded in the future with a much larger and more diverse set of information than they currently handle, which will likely bring them some kind of benefit. On the other side are projects that seek to directly benefit society and that seek to make a profit. In the era of Big Data, some projects are not entirely effective due to the lack of a truly large volume of information that allows for reliable data analysis. Being able to access wider sources of information will be a benefit. Such projects would not be able to become recognised data altruism organisations but could potentially still benefit from wider data altruism initiatives, facilitated by data subject consent and portability initiatives. These altruistic exchanges share certain features with free distribution systems regarding copyrighted works, such as Creative Commons or Copyleft licensing schemes. In both cases, the proliferation of information is based on the principles of altruism, collaboration, and the removal of restrictions for access to resources.

Under the GDPR, an informed consent form must be express and specific. It seems that this Act may allow a **more generic consent that opens the door to broader, future, purposes**. It is worthy of note that a similar provision already exists in Recital 33 of the GDPR, which recognises that it may not be possible to fully identify the purpose of particular scientific research purposes at the time of data collection and which allows consent to be given more broadly, to certain areas of scientific research, in line with recognised ethical standards.

Competition vs. Regulation: the case of the DGA

Data transfer

The Act starts **to extend restrictions on transfers of data into non-personal data**. Accordingly, while the restrictions do not apply to personal data (because the GDPR already contains similar, or more extensive, restrictions), they may still be of relevance.

Most restrictions are introduced into re-use of public sector body data. **If a re-user intends to transfer non-personal data to a third country, then it has to notify the public sector body of this at the time that it requests re-use of the data**. The public sector body, in turn, must notify the parties who may be affected by this – and may only grant the re-use request if those parties give permission for the transfer.

Where transfers are permitted, then the re-user must give contractual assurances to comply with IPR & confidentiality requirements post transfer and to accept the jurisdiction of the courts of the Member State where the public sector body is based. **The Act also introduces a possibility for the Commission to adopt model contractual clauses and to declare certain countries to offer adequate protection for non-personal data, or to introduce additional restrictions for certain categories of non-personal data which pose a high risk**. The recitals to the Act set out the types of factors which the Commission must consider when assessing the adequacy of the level of protection offered – **these will be familiar from Schrems II**.

Competition vs. Regulation: the case of the DGA

Data transfer

- So far, the non-personal data transfer restrictions may sound of limited relevance: primarily affecting public sector bodies, or those receiving data form such bodies. However, Art. 30 extends these restrictions. This **introduces a general obligation on public sector bodies, those allowed data for re-use, as well as data intermediation and data altruism organisations to take all reasonable measures to prevent international transfers of or government access to non-personal data held in the Union, where this would conflict with EU or Member State law**.
- The Act also contains a provision equivalent to GDPR Art. 48 – noting that third country judgments or decisions requiring access to data are only recognised in the EU if based on an international treaty. Further, any re-user of public sector data, an intermediation service provider and any recognised data altruism organisation who receives a third country request for non-personal data that would conflict with EU or Member State law **must provide the minimum possible data in response to such a request and may only co-operate with it**, where either the request is recognised under an international treaty etc. or where conditions set out in the Act (addressing proportionality; court authorisation; and recognition of interests protected under EU or Member State law) are met. **The provider must also notify data holder of request – unless request is for law enforcement purposes (not national security) and where this is necessary to preserve effectiveness of the law enforcement activity. Providers of intermediation services, or data altruism services, which relate to non-personal data will, therefore, have to use transfer risk assessments and processes for dealing with public authority requests to access data**.

Competition vs. Regulation: the case of the DGA

Creation of a European Data Innovation board, compliance and enforcement

The Act requires an **European Data Innovation Board**, made up of a group of experts in the field, to be created. The Board should consist of representatives of the Member States, the Commission and relevant data spaces and specific sectors (such as health, agriculture, transport and statistics). The European Data Protection Board should be invited to appoint a representative.

Member States must designate one or more competent authorities to administer the register of data altruism organisations and of data intermediaries and to enforce the legislation. These **designated competent authorities must coordinate with other authorities that may have an interest, such as data protection authorities, national competition authorities, cybersecurity authorities and other relevant sectoral authorities**.

Article 31 of the Act states that fines are to be set and implemented by each Member State. Unlike the GDPR, **the Act does not prescribe the specific amounts and weighting factors applicable to the corresponding monetary sanctions**. However, similarly to Article 83 GDPR, the Act provides that Member States must ensure that the decided penalties are "effective, proportionate and dissuasive".

Università Europea di Roma

Co-funded by the Erasmus+ Programme of the European Union

COMPETITION VS. REGULATION IN DIGITAL MARKETS

THE DIGITAL SERVICES ACT PACKAGE: THE CASE OF THE DATA ACT («DA»)

Competition vs. Regulation: the case of the DA

On 23 February 2022, the European Commission unveiled its proposal for a Data Act (DA). As declared in the Impact Assessment, the DA complements two other major instruments shaping the European single market for data, such as the Data Governance Act and the Digital Markets Act (DMA), and **is a key pillar of the European Strategy for Data in which the Commission announced the establishment of EU-wide common, interoperable data spaces in strategic sectors to overcome legal and technical barriers to data sharing**.

The DA also represents the latest effort of European policy makers to ensure free flows of data through a broad array of initiatives which differ among themselves in terms of scope and approach: some interventions are horizontal, others are sector-specific; some mandate data sharing, others envisage measures to facilitate the voluntary sharing; some introduce general data rights, others allow asymmetric data access rights.

A political agreement was reached by the European Parliament and the Council on 28 June 2023. Following its entry into force, the Data Act will become applicable in 20 months, i.e. 12 September 2025.

Competition vs. Regulation: the case of the DA

The proposed DA aims to achieve five objectives:

- **to facilitate access to and the use of data by consumers and businesses**, while preserving incentives to invest in ways of generating value through data;
- to **provide for the use by public sector bodies and EU institutions of data held by enterprises** in certain situations where there is an exceptional data need;
- to **facilitate switching between cloud and edge services**;
- to **put in place safeguards against unlawful data transfer without notification by cloud service providers**;
- and to **provide for the development of interoperability standards for data to be reused between sectors**, in a bid to remove barriers to data sharing across domain-specific common European data spaces and between other data that are not within the scope of a specific common European data space.

Competition vs. Regulation: the case of the DA

These goals reflect the main problem that the initiative detects, which is **the insufficient availability of data for use and reuse**. Notably, although the use of connected products increasingly generates data which in turn may be used as input by services that accompanied these products, **consumers and companies (especially start-ups, small and medium-sized enterprises - SMEs) have limited ability to realize the value of data generated by their use of products and related services, since they lack effective control over the data**.

In many sectors, manufacturers are often able to determine, through their control of the technical design of the product or related services, what data is generated and how it can be accessed, even though they have no legal right to the data. In situations where the data is generated by machines through the use of products and related services by businesses and consumers, it is indeed unclear whether the acquisition of an object includes the benefit of having a share in the value of the data. Legal uncertainties regard the question of the applicability of the Database Directive to machine-generated data and also pertain to the portability and interoperability of data. Moreover, with regards to data subjects, the **GDPR is considered insufficient to alleviate the problem of limited control over the data, because the right to data portability does not apply to non-personal data and it is confined to personal data processed for the performance of a contract or based on consent**. In a similar vein, sectoral legislations ensure that only in certain areas (e.g., electricity, banking, cars) third parties can have access to relevant data.

Competition vs. Regulation: the case of the DA

Finally, **data sharing within and between sectors requires an interoperability framework**. Indeed, the absence of common and compatible standards for both semantic and technical interoperability represents the main barrier to data sharing and reuse, and a very relevant problem for the effective portability of data and for switchability between cloud and edge services.

In summary, alongside the general goal of empowering users to gain and exert control over their data, the **DA is also pursuing other objectives, such as safeguarding and promoting competition, innovation, and fairness in the digital economy**.

The concept of fairness is interpreted in **broad terms and refers to the allocation of economic value from data among actors**. This concern stems from the observation that data value is concentrated in the hands of relatively few large companies, while the data produced by connected products or related services are an important input for aftermarket, ancillary and other services.

Therefore, to achieve a greater balance in the distribution of such value, the fairness of both contractual terms and market outcomes are addressed. Indeed, the creation of a cross-sectoral governance framework for data access and use aims to ensure contractual fairness, namely to rebalance the negotiation power for SMEs in data sharing contracts and prevent vendor lock-in in cloud and edge services. As a result, fairer and more competitive market outcomes shall be promoted in aftermarkets and in data processing services.

Competition vs. Regulation: the case of the DA

Such a broad notion of fairness has also been applied in the DMA and this may not be without legal risks. In the DMA, the unfairness is related to the inability of market participants to adequately capture the benefits resulting from their innovative efforts because of gatekeepers' gateway position and superior bargaining power. Moreover, contestability and fairness are considered intertwined, given that the lack of the former can enable a large player to engage in unfair practices and, similarly, unfair practices by a gatekeeper can reduce the possibility of rivals to contest its position. Concerns about fair dealing in online markets have also motivated the platform-to-business (P2B) Regulation, which noted that, given the increasing dependence of business users on online intermediation services, the providers of those services often have superior bargaining power which enables them to behave unilaterally in a way that can be unfair.

Università Europea di Roma

Co-funded by the Erasmus+ Programme of the European Union

JEAN MONNET CHAIR IN DIGITAL TRANSFORMATION AND AI POLICY

DATA REGULATIONS AND FUNDAMENTAL RIGHTS

Course Market Law and Regulation a.y. 2023-2024

Course convenor: Professor Valeria Falce (Valeria.Falce@unier.it)

Università Europea di Roma

Co-funded by the Erasmus+ Programme of the European Union

Module 3.

Università Europea di Roma

Co-funded by the Erasmus+ Programme of the European Union

DIGITAL DECADE VISION

Digital Decade Vision

The European Commission has updated the EU's digital strategy in light of the importance of digital technology for the economy and society, as the coronavirus pandemic has recently highlighted.

It builds on the 2020 strategy on shaping Europe's digital future, which remains the overarching framework, while reconsidering the enormous changes brought about by Covid-19.

The pandemic has massively accelerated the use of digital tools, demonstrating their opportunities while exposing society's vulnerability to new digital divides. In the post-coronavirus environment, the EU aims to protect and reinforce its digital sovereignty in strategic areas to ensure strategic autonomy in the digital area, while also promoting common EU values and respecting fundamental freedoms, including data protection and privacy, safety and security.

On 9 March 2021, the European Commission presented its vision for Europe's digital transformation by 2030. Its communication on the "2030 Digital Compass: the European way for the Digital Decade" announced an update of the Commission's overall digital strategy from February 2020 and of its gigabyte society targets, set in 2020 and 2016 respectively. This new strategy has been put forward to address a number of digital vulnerabilities revealed by the coronavirus crisis, such as dependency on non-European technologies. Europe should fund and support the development of sectors that are crucial to its digital sovereignty, such as semiconductors and edge computing.

The 2030 Digital Compass

The Commission has identified four main areas for action:

1 Achieve a digitally-skilled population and highly-skilled digital professionals;

2 Implement secure and performant sustainable digital infrastructures;

3 Achieve the digital transformation of businesses; and

4 Achieve the digitalization of public services.

Each of the four cardinal points of the digital compass relates to one of the four digital decade goals.

1. A digitally skilled population and highly skilled digital professionals:

At least 80% of all adults should have basic digital skills by 2030: this indicator follows the European Pillar of Social Rights action plan.

Reach 20 million employed ICT specialists in the EU, with convergence between women and men, compared to 7.8 million in 2019. Currently, more than 70 % of businesses report a lack of staff with adequate digital skills as an obstacle to investment. There is also a severe gender imbalance, with only one in six information and communication (ICT) specialists and one in three science, technology, engineering, and mathematics (STEM) graduates being women.

The 2030 Digital Compass

2. Secure and performant sustainable digital infrastructure:

By 2030, all European households should be covered by 5G, as well as by a fixed gigabit network. All European households should have gigabit connectivity compared to 59% in 2020 and all populated areas covered by 5G, up from 14 % in 2021. High performance computing (HPC) will require terabit connections to allow real-time data processing.

The production of cutting-edge and sustainable semiconductors in Europe, including processors, should represent at least 20 % of world production in value, doubling from 10 % in 2020.

10 000 climate-neutral highly secure edge nodes should be deployed in the EU and distributed in a way that guarantees access to data with low latency (i.e. few milliseconds), wherever businesses are located.

The quantum revolution in the next decade will be a game-changer in the emergence and use of digital technologies. By 2025, Europe should have its first computer with quantum acceleration, paving the way for Europe to place at the cutting edge of quantum capabilities by 2030.

The 2030 Digital Compass

3. Digital transformation of businesses:

The transformation of businesses will depend on their ability to adopt new digital technologies rapidly and across the board, including in industrial and services ecosystems that are lagging behind. Three out of four companies should use cloud computing services, big data and artificial intelligence by 2030.

More than 90 % of European SMEs should reach at least a basic level of digital intensity, compared to 61% in 2019.

Creation of around 250 unicorns (start-ups valued at US$1 billion) should be supported in the EU, a 100 % increase compared to 2021.

4. Digitalisation of public services:

All key public services should be available online.

All citizens will have access to their e-medical records.

80 % citizens should use a digital identity (ID) solution.

The 2030 Digital Compass

Figure 1 – Digital decade compass

Skills

ICT Specialists: 20 million + Gender convergence
Basic Digital Skills: min 80% of population

Public Services

Key Public Services: 100% online
e-Health: 100% availability medical records
Digital Identity: 80% citizens using digital ID

Infrastructures

Connectivity: Gigabit for everyone, 5G everywhere
Cutting edge Semiconductors: double EU share in global production
Data – Edge & Cloud: 10,000 climate neutral highly secure edge nodes
Computing: first computer with quantum acceleration

Business

Tech up-take: 75% of EU companies using Cloud/AI/Big Data
Innovators: grow scale ups & finance to double EU Unicorns
Late adopters: more than 90% of European SMEs reach at least a basic level of digital intensity

Source: European Commisssion: Europe's digital decade.

Digital principles and rights

The Commission therefore tabled a proposed **declaration on digital rights and principles for a human-centred digital transformation on 26 January 2022**, aiming at raising awareness and creating an overarching reference framework to govern this process.

The proposal builds on previous work done in this respect: the eGovernment (Tallinn Declaration), digital society and value-based digital government (Berlin Declaration), and digital democracy with a purpose (Lisbon Declaration). However, this new declaration is the first dedicated entirely to the fundamental rights of EU citizens in the digital environment.

The declaration would not be legally binding; it is an instrument to raise understanding of the EU acquis in the digital field. It derives from primary and secondary EU law and the CJEU and the European Court of Human Rights case law. The principles of the declaration are based on the EU Charter of Fundamental Rights and the EU Treaties, adapted to the digital environment. Existing fundamental rights are applied online, so that the exact same safeguards and rights for citizens are applied in the same way as offline.

Digital principles and rights

The draft declaration does not replace other proposals – instead it complements them. It also does not confer new rights; it is a collection of existing rights serving as a reference for public and private entities when dealing with new technologies and digital transformation. It is complementary to existing rights already introduced in the EU Charter on Fundamental Rights, General Data Protection Regulation (GDPR), and ePrivacy legislation, to name just a few examples. However, it introduces new issues, such as transparency of artificial intelligence (AI) algorithms – dealt with in the proposed AI act – which it compliments in this regard.

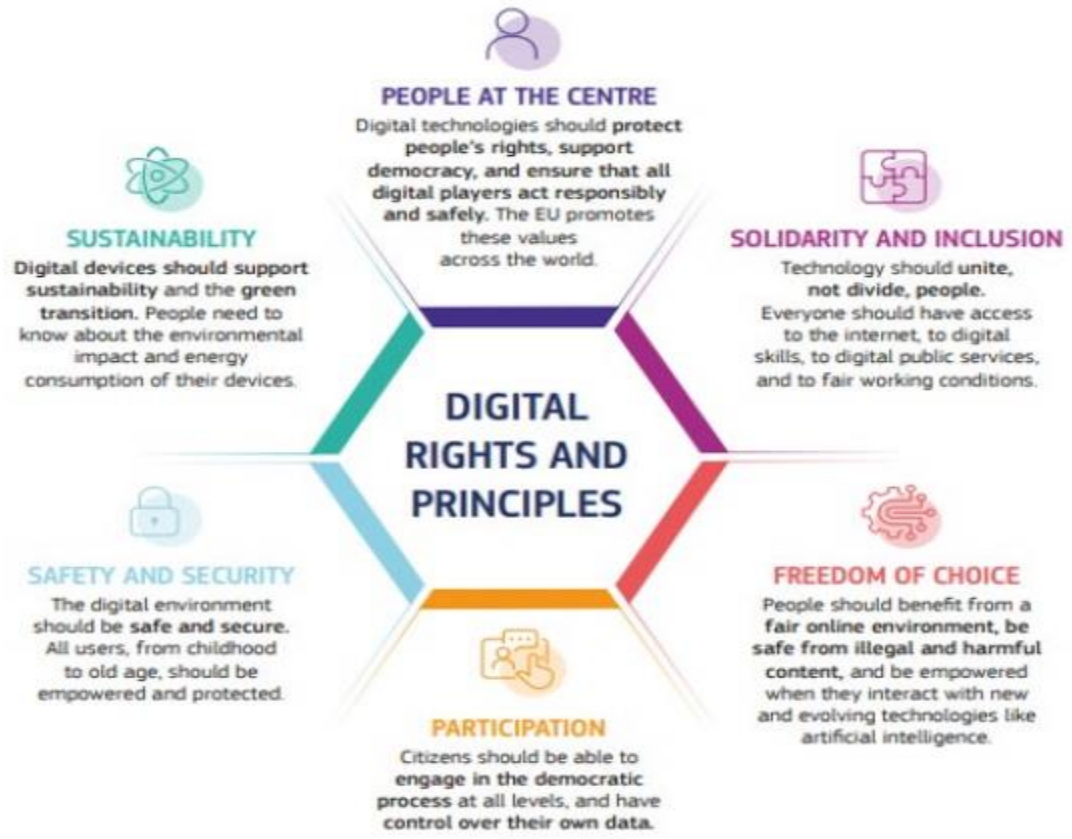
The draft declaration does not envisage direct enforcement. It however provides a framework for meeting the EU's digital decade targets and envisages an annual assessment of the digital transition.

Its adoption could however enable initiating legislation to transform rights into enforceable legal instruments. As European Commissioner Margrethe Vestager notes, the principles of the declaration provide "a blueprint for the digital transition".

As such, the proposed declaration is above all a political document, combining the policy and constitutional approaches and has primarily an advocacy role aimed at raising public awareness as well as promoting digital rights worldwide.

Digital principles and rights

Figure 2– Digital rights and principles



Source: European Commission: Digital Rights and Principles Factsheet.

Università Europea di Roma

Co-funded by the Erasmus+ Programme of the European Union

THE CASE OF THE ARTIFICIAL INTELLIGENCE ACT («AI ACT»)

The case of the AI Act

On 1 August 2024, the European Artificial Intelligence Act (AI Act) enters into force. The Act aims to foster responsible artificial intelligence development and deployment in the EU.

Proposed by the Commission in April 2021 and agreed by the European Parliament and the Council in December 2023, the AI Act addresses potential risks to citizens' health, safety, and fundamental rights. It provides developers and deployers with clear requirements and obligations regarding specific uses of AI while reducing administrative and financial burdens for businesses.

Recently, the Commission has launched a consultation on a Code of Practice for providers of general-purpose Artificial Intelligence (GPAI) models. This Code, foreseen by the AI Act, will address critical areas such as transparency, copyright-related rules, and risk management. GPAI providers with operations in the EU, businesses, civil society representatives, rights holders and academic experts are invited to submit their views and findings, which will feed into the Commission's upcoming draft of the Code of Practice on GPAI models.

The provisions on GPAI will enter into application in 12 months. The Commission expects to finalize the Code of Practice by April 2025. In addition, the feedback from the consultation will also inform the work of the AI Office, which will supervise the implementation and enforcement of the AI Act rules on GPAI.

The case of the AI Act

The EU AI Act introduces a sophisticated ‘product safety regime’ constructed around a set of 4 risk categories. It imposes requirements for market entrance and certification of High-Risk AI Systems through a mandatory CE-marking procedure. This pre-market conformity regime also applies to machine learning training, testing and validation datasets.

The AI Act combines a risk-based approach based on the pyramid of criticality, with a modern, layered enforcement mechanism. This means that as risk increases, stricter rules apply. Applications with an unacceptable risk are banned. Fines for violation of the rules can be up to 6% of global turnover for companies.

The EC aims to prevent the rules from stifling innovation and hindering the creation of a flourishing AI ecosystem in Europe, by introducing legal sandboxes that afford breathing room to AI developers.

The case of the AI Act

The EU AI Act sets out horizontal rules for the development, commodification and use of AI-driven products, services and systems within the territory of the EU. The draft regulation provides core artificial intelligence rules that apply to all industries.

The EU AI Act introduces a sophisticated ‘product safety framework’ constructed around a set of 4 risk categories. It imposes requirements for market entrance and certification of High-Risk AI Systems through a mandatory CE-marking procedure. To ensure equitable outcomes, this pre-market conformity regime also applies to machine learning training, testing and validation datasets.

The Act seeks to codify the high standards of the EU trustworthy AI paradigm, which requires AI to be legally, ethically and technically robust, while respecting democratic values, human rights and the rule of law.

CONTENTS

Co-funded by the Erasmus+ Programme of the European Union

THE NUMBERS OF THE WORLD AI MARKET

1.9 TRILLION BY 2030

According to the latest estimates provided by Statista, the global AI market has been valued at over EUR 130 billion in 2023 and is expected to grow substantially to almost EUR 1.9 trillion by 2030.

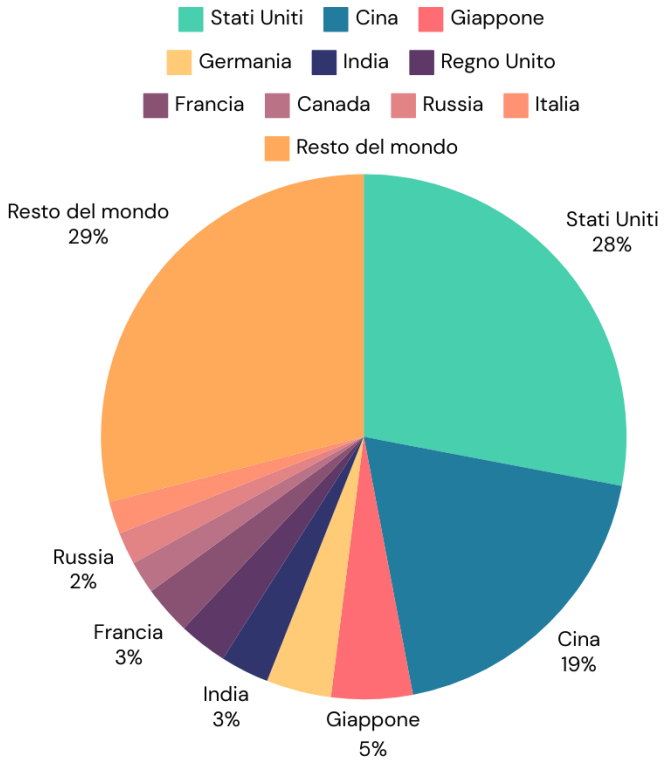
PREDOMINANCE OF PRIVATE INVESTMENT

Private investment accounts for the majority of investments in AI.

120 BILLION IN US COMPANIES

Between 2018 and the third quarter of 2023, almost EUR 32.5 billion was invested in EU AI companies, compared to more than EUR 120 billion in US AI companies.

THE WORLD AI MARKET BY COUNTRY (IN % OF TOTAL VALUE, 2024)

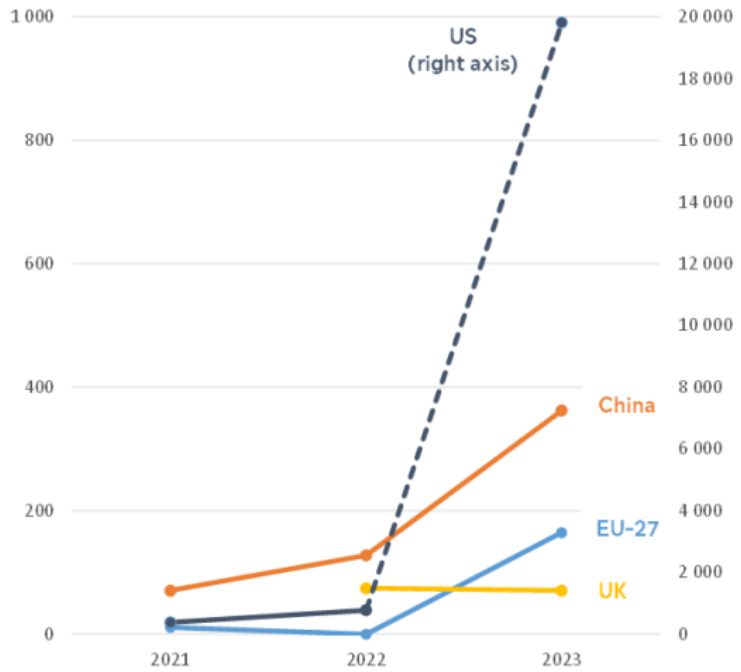


SOURCE: I-COM

PRIVATE INVESTMENT IN AI BY COUNTRY, 2023 (BILLION EURO)

Source: Stanford University, 2024 AI Index Report

VENTURE CAPITAL INVESTMENTS IN GENERATIVE A BY COUNTRY (MILLIONS OF EURO)



Source: OECD/Preqin, 2024

THE NUMBERS OF THE EUROPEAN AI MARKET

2.1 BILLION EURO INVESTMENT

Public investment in AI is growing. The EU's Digital Europe programme will fund AI with a total of EUR 2.1 billion over the period 2021-2027.

42 BILLION EURO MARKET

Statista indicates that the AI market in Europe is expected to stand at just over EUR 42 billion by the end of 2024, almost doubling the value of the market compared to 2020. The market is then expected to grow further, adding over EUR 190 billion by 2030.

ACCESS TO EUROPEAN FUNDING

In January 2024, the EU introduced measures to support European start-ups and SMEs in the development of reliable AI by granting access to funding, including the VentureEU, Horizon Europe, Digital Europe, EIC accelerator and InvestEU programmes.

THE 4 MAIN INDUSTRIAL SECTORS THAT HAVE ADOPTED AI TO DATE

As of 2023, the banking industry has seen a significant increase in AI adoption of 43%, transforming customer service, enhancing security and increasing operational efficiency. Financial institutions now leverage AI to provide tailored banking experiences and implement sophisticated fraud detection systems.

The IT sector, with an AI adoption rate of 13.8 per cent, is a crucial driver of AI integration, especially in areas such as cybersecurity, data analytics and software development. In addition to infrastructure, AI drives advances in cloud computing, data privacy and user experience.

The integration of AI in healthcare has significantly transformed medical diagnostics. Algorithms analyse medical images with greater speed and accuracy, aiding doctors in the early diagnosis of diseases. By processing large data sets, AI identifies patterns not noticed by humans.

An AI adoption rate of 12 per cent indicates the advent of smart manufacturing, characterised by AI-driven robotics, predictive maintenance and optimised supply chains. AI leads to greater efficiency and sustainable practices, highlighting its transformative role in manufacturing.

THE EUROPEAN APPROACH TO AI

The European approach to AI is inspired by two principles: technological sovereignty for strategic autonomy and the centrality of people in digital transformation. The objective is twofold: enhancing research and industrial capacity while guaranteeing fundamental rights.

However, the EU remains a secondary player in the development of AI and suffers from chronic delays in innovation. Lack of investment, incomplete single market, unattractiveness for talent, data scarcity, and regulatory complexity hinder the EU's emergence as a technological powerhouse.

A second major brake is the absence of an innovation ecosystem for European AI excellence. Among the 20 largest tech companies, only three are European (Accenture, SAP and ASML).

THE EUROPEAN STRATEGY ON AI

The Commission's AI strategy was launched with the adoption of the communication 'Artificial Intelligence for Europe' in April 2018.

The main assumption behind the strategy is that Europe can lead the way in the development and use of AI for the benefit of all, building on its values and strengths.

The European AI strategy is based on three distinct but complementary commitments:

- Increase investment to a level that matches the economic weight of the European Union;
- Leave no one behind - with particular reference to education - and ensure a smooth transition to the AI era in the workplace;
- Ensure that new technologies reflect European values.

THE TURNING POINT OF THE EU AI STRATEGY

The EU's AI le strategy reached a turning point in December 2019 with the arrival of the new European Commission led by Ursula von der Leyen. Following the appointment of Thierry Breton as Commissioner for the Single Market, the Commission also intensified its efforts on the European Data Strategy.

IOn 19 February 2020, the Commission launched a comprehensive package containing its ideas and actions on digital transformation, including a White Paper on Artificial Intelligence and a European Data Strategy.

The package marks another step forward in Europe's quest for ‘human-centric’ AI.

A EUROPEAN APPROACH TO AI

In 2021, the Commission is publishing a Communication on the promotion of a European approach to artificial intelligence.

The Communication includes 4 main objectives:

- Establish favourable conditions for the development and adoption of AI in the EU;
- Make the EU the place where excellence thrives ‘from the lab to the market’;
- Ensure that AI serves people as well as being a positive factor for society;
- Establishing strategic leadership in high-impact areas.

OBJECTIVE 1

Establishing favourable conditions for the development and adoption of AI in the EU

- Acquiring, pooling and sharing strategic information
- Exploiting the potential of data
- Promoting critical computing skills

OBJECTIVE 2

Making the EU the place where excellence thrives 'from the lab to the market'

- Collaborate with stakeholders, e.g. the European Partnership on AI, Data and Robotics and expert groups
- Build and mobilise research capacity
- Provide an environment in which developers can test and experiment and SMEs and P.A. can adopt AI
- Fund and scale up innovative AI ideas and solutions

OBJECTIVE 3

Ensuring that AI serves people

- Cultivate talent and improve the supply of skills needed to enable a thriving AI ecosystem
- Develop a strategic framework to ensure trust in AI systems
- Promote the EU's vision for sustainable and trusted AI to the world

OBJECTIVE 4

Establishing strategic leadership in high impact sectors

- Using AI in climate and environment
- Using the next generation of AI to improve health
- Preserving Europe's leadership: A strategy for robotics in the AI world

THE EU AI ACT

APRIL 2021

In April 2021, with a risk-based approach, the Commission presented its proposal for a ‘future-proof’ Artificial Intelligence Act, which establishes horizontal rules on AI, focusing on damage prevention.

MARCH 2024

On 13 March 2024, the European Parliament passed the AI Act, which became the world's first AI regulation.

MAY 2024

On 20 May 2024, the EU Council gave final approval to the AI Act, which will enter into force twenty days after its publication in the EU Official Journal.

JULY 2024

On 12 July 2024, the Artificial Intelligence Act, (Regulation (EU) 2024/1689) was published in the EU Official Journal.

Co-funded by the Erasmus+ Programme of the European Union

KEY OBJECTIVES (ART. 1; RECITALS 1-8)

- "Improve the functioning of the internal market by laying down a uniform legal framework" for the development, placing on the market, commissioning and use of AI systems in the EU.
- "Promote the deployment of human-centric and trustworthy artificial intelligence", centred on respect for EU values, ensuring a high level of protection of health, safety, the environment, democracy, the rule of law and the fundamental rights enshrined in the Charter (set out in recital 48).
- Preventing and mitigating the risks of AI by prohibiting or restricting the use of AI systems that present unacceptable risks to the safety, health, dignity or autonomy of individuals, or that violate democratic values.
- Supporting innovation, with a focus on SMEs, including start-ups, by providing priority access to regulatory sandboxes, reduced fees for conformity assessment and simplified forms for technical documentation for high-risk AI systems.

SCOPE OF APPLICATION (ART. 2; RECITALS 22, 24, 25)

- The AI Act does not apply to areas outside the scope of EU law.
- The regulation will not apply to AI systems that have “military, defence or national security purposes, regardless of the type of entity carrying out these activities”, nor to AI systems used exclusively for research and innovation purposes, nor to persons using AI for non-professional purposes.
- The regulation will apply to deployers of AI systems who place such systems on the EU market, as well as to operators, even if located outside the EU, if the output produced by the AI system is used in the EU.
- Importers, distributors, manufacturers and authorised representatives of AI systems are also included in the scope. Systems used in commercial activities, systems addressed to natural persons, both embedded and stand-alone systems.

AI SYSTEM (ART. 3(1); RECITAL 12)

- Automated ("machine-based system").
- Designed to operate with varying levels of autonomy.
- Can exhibit "adaptability to learn new, distinct tasks" after deployment, i.e. ability to change during use (due to self-learning).
- Characterised by inferential capacity, i.e. the "capability to derive models or algorithms, or both, from inputs or data", to generate from the input it receives, for implicit or explicit purposes*, outputs, content, predictions, recommendations or decisions capable of influencing physical or virtual environments. Inference is possible through the use of machine learning techniques and logic and knowledge-based approaches in the construction of the system.

*Explicit goals: encoded by the developer directly in the system;

*Implicit goals: underlying human-specified rules or embedded in training data and derived through learning processes (e.g. LLM).

WHY DID THE EU LEGISLATOR DRAFT SUCH DEFINITION OF AI SYSTEM?

- Simple, broad and flexible definition, aligned with the definition adopted at the OECD (see Explanatory Memorandum No. 8, March 2024) to ensure legal certainty and facilitate international convergence.

- Focus on functional characteristics of the system, not on technical specifications and development methodologies, to ensure flexibility to facilitate rapid technological developments. This does not include traditional software, simpler programming approaches, systems that automatically perform operations according to predefined human rules (i.e. static or deterministic ‘if-then’ programming, as opposed to dynamic-probabilistic programming).

- The Commission will develop guidelines on the application of the definition.

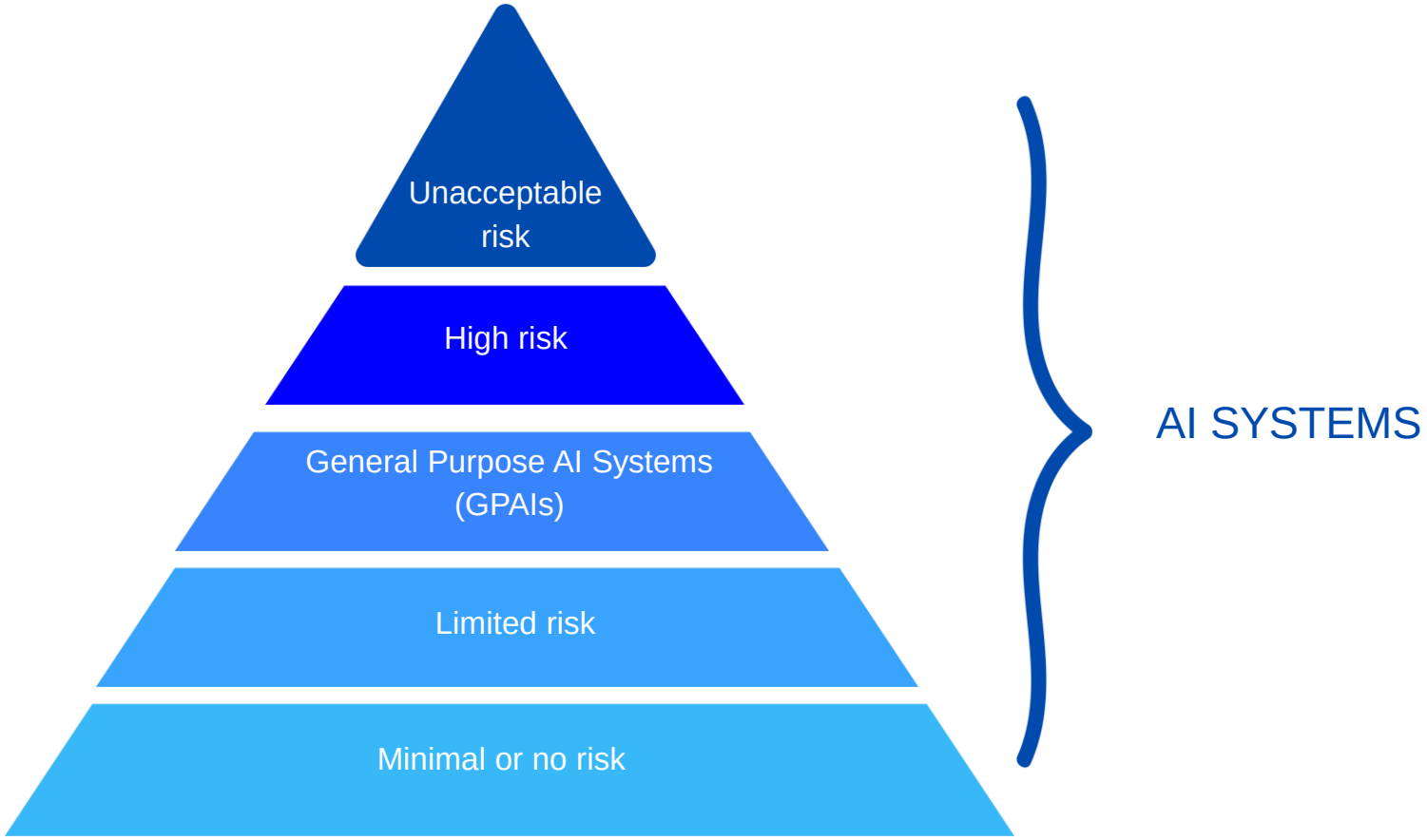
THE RISK-BASED APPROACH (RECITAL 26)

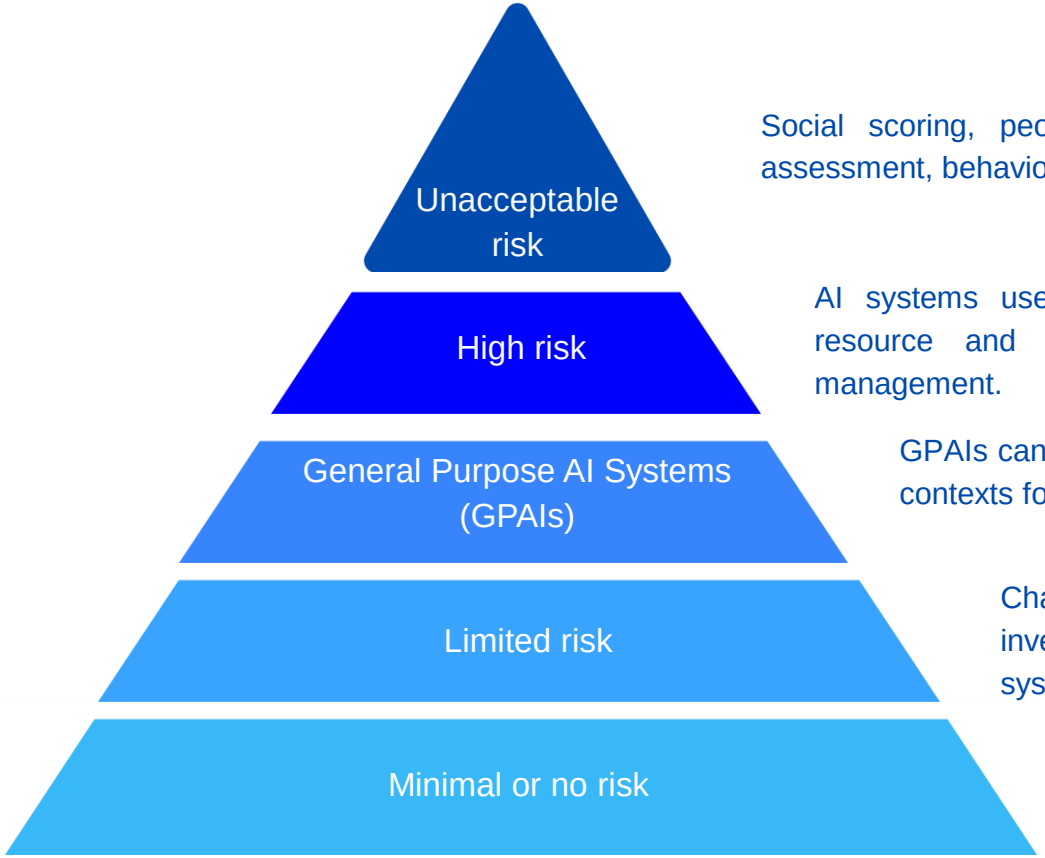
- Unacceptable risk: prohibited AI practices (Art. 5). Example: social scoring, biometric recognition, emotion assessment, behaviour prediction, trawling of people's images.

- High risk: compliance requirements, ex ante compliance assessment and obligations for operators (Art. 6-49). Example: AI systems used in medical devices, recruitment tools, human resources and workers management and critical infrastructure management.

- Specific risks related to deception or impersonation: transparency obligations for operators, possibly in addition to those for high-risk systems (Art. 50). Example: chatbots, deepfakes, AI-enabled video games, inventory management systems, market segmentation systems.

- Minimal or no risk: no specific obligation, but duty of literacy (Art. 4) and voluntary adherence to codes of conduct (Art. 95). The codes provide the same obligations for providers of general purpose AI models.


Unacceptable risk
High risk
General Purpose AI Systems (GPAIs)
Limited risk
Minimal or no risk
AI SYSTEMS



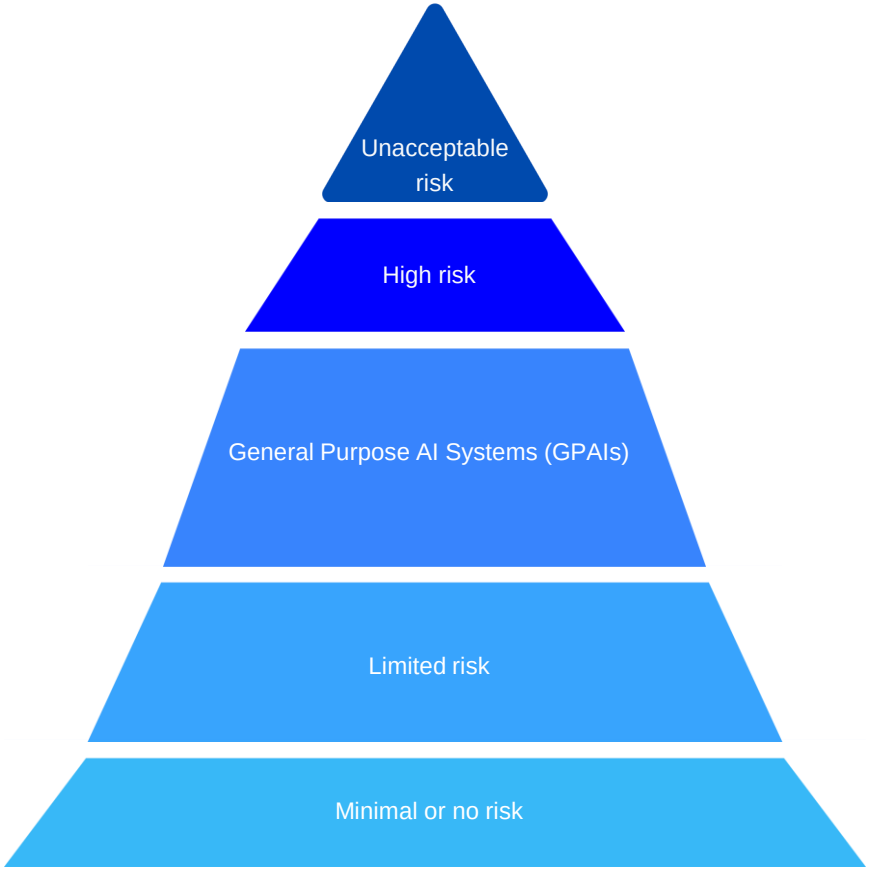
Social scoring, people manipulation, biometric recognition, emotion assessment, behaviour prediction, image trawling of people.

AI systems used in medical devices, recruitment tools, human resource and worker management and critical infrastructure management.

GPAIs can be used or adapted to a wide number of application contexts for which they were not specifically designed.

Chatbots, deepfakes, AI-enabled video games, inventory management systems, market segmentation systems.

All AI systems not included in the other categories.



An AI system that poses an unacceptable risk because it violates the fundamental rights of end users is prohibited throughout the EU.

The provider of a high-risk AI system must comply with requirements (Arts. 6 - 49), including subjecting the system to a conformity assessment before placing it on the market.

The provider of GPAIs is required to comply with transparency requirements (Art. 53), including the disclosure of certain information to downstream system providers. Additional obligations exist for GPAI systems that pose 'systemic risks', including GPAIs trained using computing power exceeding 10^25 FLOPs, such as GPT-4.

The provider of a low-risk AI system, including AI systems for general low-impact purposes (such as chatbots and deepfakes), must comply with specific transparency obligations (Art. 50), which include, for example, ensuring that users are aware that they are interacting with an AI.

Providers of AI systems that present a low or minimal risk to the security and fundamental human rights of end users are encouraged to voluntarily comply with mandatory requirements for high-risk AI systems through voluntary codes of practice.

AI MODELS FOR GENERAL PURPOSES OR GPAI (ART. 3(63); RECITALS 97-99)

Usually trained on large amounts of data by various methods, such as self-supervised, unsupervised or reinforcement-based learning, it is characterised by:

- significant generality;
- ability to competently perform a wide range of distinct tasks;
- suitability to be integrated into a variety of downstream systems or applications.

GPAI models are certainly those with at least one billion parameters and trained by means of large-scale self-supervision (recital 98), especially large generative AI models (recital 99).

The regulation applies to GPAI models once they have been placed on the market (regardless of the mode), not to those used before they are placed on the market for research, development and prototyping purposes only.

Providers and deployers of AI systems with limited risk, including general purpose AI systems with low impact, must comply with a number of transparency obligations regulated in Art. 50.

SYSTEMIC GPAI MODELS (ART. 3(65), ART. 51; RECITAL 110)

Due to their high impact capacity, they may pose a systemic risk that significantly affects the EU market due to their scale and with actual or reasonably foreseeable negative effects on public health, security, fundamental rights or society as a whole, which may propagate along the entire value chain.

According to Art. 51 and recitals 111-113, systemic GPAIs are classified as those that:

- have high impact capabilities assessed on the basis of appropriate technical tools and methodologies (notification procedure) or;
- are designated as such by an individual decision of the Commission, based on the criteria set out in an annex to the AI Act.

High impact capacity presumed if FLOP greater than 10^25. This threshold will be reviewed by the Commission in the light of technological developments.

GPAI SYSTEMS (ART. 3, PARA. 66; RECITAL 100)

- based on a GPAI model;
- because of this integration, it has the capacity to serve various purposes, either for direct use or for integration into other AI systems.

Recital 85

"General-purpose AI systems may be used as high-risk AI systems by themselves or be components of other high-risk AI systems. Therefore, due to their particular nature and in order to ensure a fair sharing of responsibilities along the AI value chain, the providers of such systems should, irrespective of whether they may be used as high-risk AI systems as such by other providers or as components of high-risk AI systems and unless provided otherwise under this Regulation, closely cooperate with the providers of the relevant high-risk AI systems to enable their compliance with the relevant obligations under this Regulation and with the competent authorities established under this Regulation."

TRANSPARENCY OBLIGATIONS FOR GPAI SYSTEMS (ART. 53; RECITAL 101)

In addition to the transparency obligations set out in Art. 50, providers of general purpose AI systems, general purpose AI models and generative AI must comply with a number of result obligations set out in Art. 53.

TRANSPARENCY OBLIGATIONS GPAI SYSTEMS, GPAI MODELS AND GENERATIVE AI (ART. 53; RECITAL 101)

In addition to the transparency obligations set out in Art. 50, providers of general purpose AI systems, general purpose AI models and generative AI must comply with a number of result obligations set out in Art. 53.

Recital 101

“Providers of general-purpose AI models have a particular role and responsibility along the AI value chain, as the models they provide may form the basis for a range of downstream systems, often provided by downstream providers that necessitate a good understanding of the models and their capabilities, both to enable the integration of such models into their products, and to fulfil their obligations under this or other regulations. Therefore, proportionate transparency measures should be laid down, including the drawing up and keeping up to date of documentation, and the provision of information on the general-purpose AI model for its usage by the downstream providers. Technical documentation should be prepared and kept up to date by the general-purpose AI model provider for the purpose of making it available, upon request, to the AI Office and the national competent authorities. The minimal set of elements to be included in such documentation should be set out in specific annexes to this Regulation. The Commission should be empowered to amend those annexes by means of delegated acts in light of evolving technological developments.”

PROHIBITIONS: PROTECTED VALUES, INCIDENCE OF RISK

- Freedom of choice, self-determination: subliminal, manipulative and vulnerability-exploiting techniques capable of significantly altering the decision-making capacity and distorting the behaviour of individuals or groups (with actual or potential serious harm).

- Non-discrimination: social scoring systems with disproportionate prejudicial effect (and/or based on data acquired in other contexts); biometric categorisation to infer or deduce ‘sensitive’ characteristics of individuals; recognition of emotions in the context of work or education (characterised by power imbalance).

- Rule of law and presumption of innocence: predictive systems of criminal risk based on profiling of individuals.

- Privacy, personal data protection: image scraping to create facial recognition databases (increasing the sense of mass surveillance); real-time remote biometric identification in publicly accessible spaces for law enforcement purposes.

It is not necessary for the provider or deployer to have the intent to cause significant harm, as long as the harm results from the manipulation/exploitation made possible by the AI.

THE PROHIBITIONS IN DETAIL (ART. 5; RECITALS 29, 30, 31, 42, 43, 44)

It is prohibited to place on the market, putting into service or use:

(a) an AI system that deploys subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective, or the effect of materially distorting the behaviour of a person or a group of persons by appreciably impairing their ability to make an informed decision, thereby causing them to take a decision that they would not have otherwise taken in a manner that causes or is reasonably likely to cause that person, another person or group of persons significant harm;

(b) an AI system that exploits any of the vulnerabilities of a natural person or a specific group of persons due to their age, disability or a specific social or economic situation, with the objective, or the effect, of materially distorting the behaviour of that person or a person belonging to that group in a manner that causes or is reasonably likely to cause that person or another person significant harm;

THE PROHIBITIONS IN DETAIL (ART. 5; RECITALS 29, 30, 31, 42, 43, 44)

It is prohibited to place on the market, putting into service or use:

(c) AI systems for the evaluation or classification of natural persons or groups of persons over a certain period of time based on their social behaviour or known, inferred or predicted personal or personality characteristics, with the social score leading to either or both of the following:

(i) detrimental or unfavourable treatment of certain natural persons or groups of persons in social contexts that are unrelated to the contexts in which the data was originally generated or collected;

(ii) detrimental or unfavourable treatment of certain natural persons or groups of persons that is unjustified or disproportionate to their social behaviour or its gravity.

THE PROHIBITIONS IN DETAIL (ART. 5; RECITALS 29, 30, 31, 42, 43, 44)

It is prohibited to place on the market, putting into service or use:

(d) an AI system for making risk assessments of natural persons in order to assess or predict the risk of a natural person committing a criminal offence, based solely on the profiling of a natural person or on assessing their personality traits and characteristics; this prohibition shall not apply to AI systems used to support the human assessment of the involvement of a person in a criminal activity, which is already based on objective and verifiable facts directly linked to a criminal activity;

(Tools for analysing the risks of financial fraud by companies on the basis of suspicious transactions or aimed at locating narcotic drugs or illicit goods by customs authorities are not affected by the ban).

(e) AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage;

.

THE PROHIBITIONS IN DETAIL (ART. 5; RECITALS 29, 30, 31, 42, 43, 44)

It is prohibited to place on the market, putting into service or use:

(f) AI systems to infer emotions of a natural person in the areas of workplace and education institutions, except where the use of the AI system is intended to be put in place or into the market for medical or safety reasons;

(g) biometric categorisation systems that categorise individually natural persons based on their biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation; this prohibition does not cover any labelling or filtering of lawfully acquired biometric datasets, such as images, based on biometric data or categorizing of biometric data in the area of law enforcement;

(The labelling/filtering, on the basis of biometric data, of legally acquired datasets and the categorisation of biometric data in the field of law enforcement are excluded from the prohibition).

THE PROHIBITIONS IN DETAIL (ART. 5; RECITALS 29, 30, 31, 42, 43, 44)

It is prohibited to place on the market, putting into service or use:

(h) 'real-time' remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement, unless and in so far as such use is strictly necessary for one of the following objectives:

(i) the targeted search for specific victims of abduction, trafficking in human beings or sexual exploitation of human beings, as well as the search for missing persons;

(ii) the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or a genuine and present or genuine and foreseeable threat of a terrorist attack;

(iii) the localisation or identification of a person suspected of having committed a criminal offence, for the purpose of conducting a criminal investigation or prosecution or executing a criminal penalty for offences referred to in Annex II and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least four years.

Point (h) of the first subparagraph is without prejudice to Article 9 of Regulation (EU) 2016/679 for the processing of biometric data for purposes other than law enforcement.

‘REAL-TIME’ REMOTE BIOMETRIC IDENTIFICATION SYSTEMS IN DETAIL (ART. 5, LETTER H; RECITALS 33-34)

Real-time remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement are prohibited except as necessary to search for victims of certain crimes or missing persons, prevent imminent threats to life or limb or terrorist attacks, locate or identify suspected perpetrators of specific serious crimes, and provided that:

- the use is intended only to confirm the identity of a specific person;
- the conditions and safeguards provided for by national law are respected;
- the law enforcement authority has carried out a fundamental rights impact assessment and registered the system in the EU database;
- the use is authorised in advance by a court or an independent administrative authority (except in cases of urgency), expressly provided for by national rules, notified to the market surveillance authority and the data protection authority.

CLASSIFICATION RULES FOR HIGH-RISK AI SYSTEMS (ART. 6(1-2); RECITALS 46-52)

- Systems intended to be used as “a safety component of a product, or the AI system is itself a product” subject to harmonised EU standards (including machinery, toys, lifts, radio equipment, medical and safety devices, motor vehicles, unmanned aircraft) and subject to related ex ante conformity assessment by third parties.

- Safety component that performs a safety function for the product or whose failure or malfunction endangers the health and safety of persons or property.

- “Stand-alone” systems identified in Annex III with reference to specific sectors: biometrics; critical infrastructure; education and vocational training; employment, management of workers and access to self-employment; access to and use of essential private services and public services; law enforcement; migration, asylum and border control management; administration of justice and democratic processes.

EXCEPTIONS (ART. 6(3); RECITAL 53)

AI systems listed in Annex III that do not pose a significant risk of harm to health, safety or fundamental rights of natural persons are not considered high-risk (unless they involve profiling) because they are intended to:

- perform only a “narrow procedural task” (e.g. categorisation of documents);
- “improve the result of a previously completed human activity” (e.g. improve the language of already drafted documents);
- “detect decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously completed human assessment, without proper human review”;
- “perform a preparatory task for an assessment relevant for the purposes of the use cases listed in Annex III” (e.g. intelligent file management solutions, translation of documents).

The provider shall carry out and document the assessment prior to placing on the market/commissioning and provide documentation to the competent authorities upon request.

SOME HIGH-RISK STAND-ALONE AI SYSTEMS

Biometrics (provided use is permitted under EU or national law)

- remote biometric identification systems, if not prohibited under Art. 5. Not high-risk those used for biometric verification or authentication (e.g. allowing access to a location or unlocking a device);
- systems for biometric categorisation based on sensitive data, if not prohibited under Art. 5 (i.e. not intended to infer or deduce race, political opinions, etc.);
- systems for emotion recognition, if not prohibited under Art. 5 (i.e. used in contexts other than work and education).

Critical infrastructure

- Systems operating as security components in the management and operation of critical digital infrastructure, road traffic, water/gas/heating/electricity supply (e.g., water pressure monitoring or fire control in cloud computing centres) Security components are not those used for cybersecurity purposes only.

SOME HIGH-RISK STAND-ALONE AI SYSTEMS

Jobs

- systems for recruiting or selecting individuals, in particular for publishing targeted job advertisements, analysing or filtering applications and evaluating candidates;

- systems for making decisions concerning the conditions of employment relationships, the promotion or termination of employment relationships, for assigning tasks on the basis of individual behaviour or personal traits and characteristics, or for monitoring and evaluating people's performance and behaviour in the context of such employment relationships.

They can have a significant impact on the future of individuals in terms of career and livelihood prospects and workers' rights, perpetuate historical patterns of discrimination, and undermine fundamental rights to data protection and privacy.

Co-funded by the Erasmus+ Programme of the European Union

SOME HIGH-RISK STAND-ALONE AI SYSTEMS

Essential public and private services and benefits

- systems for assessing, by or on behalf of public authorities, the eligibility of natural persons for essential public assistance benefits and services and for granting, reducing, withdrawing or recovering such benefits and services;
- systems to assess the creditworthiness of natural persons or to establish their credit score (excluding systems used to detect financial fraud and for prudential purposes to calculate the capital requirements of banks and insurance companies);
- systems to assess risks and determine prices in relation to natural persons in the case of life and health insurance;
- systems for assessing and classifying emergency calls made by natural persons, dispatching or prioritising emergency first aid services or triaging patients in emergency health care.

SOME HIGH-RISK STAND-ALONE AI SYSTEMS

Risk Management (Art. 9, para. 65)

Establishment, implementation, documentation and maintenance throughout the life cycle of the system, with constant and systematic updating, of a risk management system that includes:

- identification and analysis of risks a) known and reasonably foreseeable arising from use in accordance with the intended purpose, b) that may arise from reasonably foreseeable misuse (human behaviour, recital 65) of the system, c) that emerge from post-market monitoring (also based on data provided by the deployer).

- adoption of appropriate and targeted risk management measures, such as to ensure, as appropriate, the elimination, reduction, mitigation or control of risks (if not eliminable, they must become ‘acceptable’) and to ensure that the deployer has the necessary information/instructions for use and training to understand the operation of the system.

MANDATORY REQUIREMENTS FOR HIGH-RISK AI SYSTEMS

Data and data governance (Art. 10, recitals 67-70)

- "Training, validation and testing data sets shall be subject to data governance and management practices appropriate for the intended purpose of the high-risk AI system". This covers in particular: design choices, data collection processes, data preparation operations, assessment of the adequacy of available datasets, evaluation of possible biases and measures to mitigate them), to ensure the high quality of training, validation and testing datasets.

- "Training, validation and testing data sets shall be relevant, sufficiently representative, and to the best extent possible, free of errors and complete in view of the intended purpose".

If personal data are involved, minimisation, privacy by design and privacy by default must be ensured, in particular by anonymisation and encryption techniques (recital 69). Exceptionally, if strictly necessary to detect and correct bias, the processing of special categories of personal data is allowed, with stringent security measures.

MANDATORY REQUIREMENTS FOR HIGH-RISK SYSTEMS

Technical documentation and record-keeping (Artt. 11-12; recital 71)

- Preparation (prior to placing on the market or putting into service) and updating of clear and comprehensible technical documentation necessary to demonstrate the conformity of the system with the requirements, to be made available to competent authorities and notified bodies. This implies a high level of competence within companies.

- SMEs, including start-ups, can provide in a simplified manner the elements of the technical documentation specified in Annex IV.

- Minimum content in Annex IV: general description of the system, detailed description of the development process (algorithms, data training, validation and testing procedures, cybersecurity measures, etc.), information on monitoring, operation and control, description of the risk management system, etc. The Commission will develop a simplified technical documentation form for SMEs.

- Design to ensure at technical level the automatic logging of events (logs) for the entire life cycle of the system (and thus traceability of operation and use by the deployer).

MANDATORY REQUIREMENTS FOR HIGH-RISK AI SYSTEMS

Transparency and provision of information to deployers (Art. 13; recital 72)

- Design and development to ensure transparency of operation and to help deployers interpret the system output and use it properly;
- Provision of instructions “for use in an appropriate digital format or otherwise that include concise, complete, correct and clear information that is relevant, accessible and comprehensible to deployers”.
- Information should include system characteristics, capabilities and performance limitations (including known or foreseeable circumstances that may entail risks, including the action of the deployer that may influence system behaviour and performance), planned human oversight measures, computational and hardware resources required for the proper functioning of the system. Where appropriate, include illustrative examples in the instructions, e.g. on limitations and intended and prohibited uses of the AI system.

Co-funded by the Erasmus+ Programme of the European Union

MANDATORY REQUIREMENTS FOR HIGH-RISK AI SYSTEMS

Human oversight (Art. 14; recital 73)

- Design and development conducted so as to ensure human supervision during use/operation and to prevent or minimise risks.
- Ensure inherent operational constraints that the system cannot override and that the system is responsive to the human supervisor.
- Measures should be identified by the provider prior to marketing or commissioning and either integrated upstream into the system or deferred for implementation by the deployer.

MANDATORY REQUIREMENTS FOR HIGH-RISK AI SYSTEMS

Human oversight details (Art. 14, par. 4)

Supervisors must be able to: (a) properly understand the relevant capacities and limitations of the high-risk AI system and be able to duly monitor its operation, including in view of detecting and addressing anomalies, dysfunctions and unexpected performance; (b) to remain aware of the possible tendency of automatically relying or over-relying on the output produced by a high-risk AI system (automation bias), in particular for high-risk AI systems used to provide information or recommendations for decisions to be taken by natural persons; (c) to correctly interpret the high-risk AI system's output, taking into account, for example, the interpretation tools and methods available; (d) to decide, in any particular situation, not to use the high-risk AI system or to otherwise disregard, override or reverse the output of the high-risk AI system; (e) to intervene in the operation of the high-risk AI system or interrupt the system through a 'stop' button or a similar procedure that allows the system to come to a halt in a safe state.

MANDATORY REQUIREMENTS FOR HIGH-RISK AI SYSTEMS

Human oversight (Art. 14; recital 73)

For high-risk AI systems referred to in point 1(a) of Annex III, the measures referred to in paragraph 3 of this Article shall be such as to ensure that, in addition, no action or decision is taken by the deployer on the basis of the identification resulting from the system unless that identification has been separately verified and confirmed by at least two natural persons with the necessary competence, training and authority. The requirement for a separate verification by at least two natural persons shall not apply to high-risk AI systems used for the purposes of law enforcement, migration, border control or asylum, where Union or national law considers the application of this requirement to be disproportionate.

MANDATORY REQUIREMENTS FOR HIGH-RISK AI SYSTEMS

Accuracy, robustness and cybersecurity (Art. 15; recitals 74-78)

- Design and development conducted so as to achieve an adequate level of accuracy, robustness (resilience against errors, failures, inconsistencies) and cybersecurity (resilience to malicious attacks by unauthorised third parties). The Commission will promote the development of benchmarks and measurement methodologies. The instructions for use will specify accuracy levels and metrics.

- Adoption of technical and organisational measures and technical redundancy solutions (back-up or fail-safe plans). For continuously learning systems, measures to avoid feedback loops.

- Cybersecurity solutions include measures to prevent and control data poisoning or model poisoning, confidentiality attacks, etc. A system that complies with the essential requirements of the EU cybersecurity regulation is considered adequate from a cybersecurity perspective.

VALUE CHAIN AND OPERATORS' OBLIGATIONS

Provider (Art. 3 (3): a natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge.

The following are subject to the AI Act (Art. 2, para. 1 a-c):

- providers placing on the market or putting into service AI systems or placing on the market general-purpose AI models in the Union, irrespective of whether those providers are established or located within the Union or in a third country;
- providers and deployers of AI systems that have their place of establishment or are located in a third country, where the output produced by the AI system is used in the Union;

VALUE CHAIN AND OPERATORS OBLIGATIONS

Obligations of providers of high-risk AI systems (Arts. 16-22; recital 81)

(a) ensure that their high-risk AI systems are compliant with the requirements set out in Section 2;
(b) indicate on the high-risk AI system or, where that is not possible, on its packaging or its accompanying documentation, as applicable, their name, registered trade name or registered trade mark, the address at which they can be contacted;
(c) have a quality management system in place which complies with Article 17;
(d) keep the documentation referred to in Article 18;
(e) when under their control, keep the logs automatically generated by their high-risk AI systems as referred to in Article 19;
(f) ensure that the high-risk AI system undergoes the relevant conformity assessment procedure as referred to in Article 43, prior to its being placed on the market or put into service;
(g) draw up an EU declaration of conformity in accordance with Article 47;
(h) affix the CE marking to the high-risk AI system or, where that is not possible, on its packaging or its accompanying documentation, to indicate conformity with this Regulation, in accordance with Article 48;
(i) comply with the registration obligations referred to in Article 49(1);
(j) take the necessary corrective actions and provide information as required in Article 20;
(k) upon a reasoned request of a national competent authority, demonstrate the conformity of the high-risk AI system with the requirements set out in Section 2;
(l) ensure that the high-risk AI system complies with accessibility requirements in accordance with Directives (EU) 2016/2102 and (EU) 2019/882.

VALUE CHAIN AND OPERATORS' OBLIGATIONS

Main obligations on provider of high-risk AI systems (Artt. 16-22; recital 81)

- keep - for 10 years after placing on the market or putting into service - and make available to the authorities all technical documentation relating to conformity with requirements, the quality management system and the EU declaration of conformity, as well as any documents issued by notified bodies
- keep (for a period appropriate to the purpose of the system, not less than six months) the logs automatically generated by the system, if under their control, and give access to them to the national authority upon request;
- ensure that before the system is placed on the market/commissioned, it undergoes a conformity assessment procedure (Art. 43), based on internal control by the provider or the involvement of notified bodies (see below);
- draw up an EU declaration of conformity (Art. 47), attesting the fulfilment of the mandatory requirements and by which the provider assumes responsibility for the conformity of the system.

VALUE CHAIN AND OPERATORS' OBLIGATIONS

Main obligations on provider of high-risk AI systems (Artt. 16-22; recital 81)

- affix the CE marking on the system (or packaging/accompanying documents), which allows free circulation in the internal market (Art. 48)
- register the system in the EU database of systems aiAnnex III;
- take the necessary corrective measures immediately (and inform distributors, importers and deployers) if they consider that the system is not in conformity, investigate the causes and inform the authorities;
- demonstrate the conformity of the system upon reasoned request by a national authority and cooperate by providing information and documentation;
- ensure that the system complies with the accessibility requirements of EU regulations for the protection of persons with disabilities;
- if established in third countries, appoint an authorised representative and specify their tasks in a written mandate.

POST-MARKETING MONITORING

Post-market monitoring by providers and post-market monitoring plan for high-risk AI system (Art. 72)

- Providers shall establish and document a post-market monitoring system in a manner that is proportionate to the nature of the AI technologies and the risks of the high-risk AI system.
- The post-market monitoring system shall actively and systematically collect, document and analyse relevant data which may be provided by deployers or which may be collected through other sources on the performance of high-risk AI systems throughout their lifetime, and which allow the provider to evaluate the continuous compliance of AI systems with the requirements set out in Chapter III, Section 2. Where relevant, post-market monitoring shall include an analysis of the interaction with other AI systems. This obligation shall not cover sensitive operational data of deployers which are law-enforcement authorities.
- The post-market monitoring system shall be based on a post-market monitoring plan. The post-market monitoring plan shall be part of the technical documentation referred to in Annex IV. The Commission shall adopt an implementing act laying down detailed provisions establishing a template for the post-market monitoring plan and the list of elements to be included in the plan by 2 February 2026. That implementing act shall be adopted in accordance with the examination procedure referred to in Article 98(2).

POST-MARKETING MONITORING

Post-market monitoring by providers and post-market monitoring plan for high-risk AI system (Art. 72)

- For high-risk AI systems covered by the Union harmonisation legislation listed in Section A of Annex I, where a post-market monitoring system and plan are already established under that legislation, in order to ensure consistency, avoid duplications and minimise additional burdens, providers shall have a choice of integrating, as appropriate, the necessary elements described in paragraphs 1, 2 and 3 using the template referred in paragraph 3 into systems and plans already existing under that legislation, provided that it achieves an equivalent level of protection.

The first subparagraph of this paragraph shall also apply to high-risk AI systems referred to in point 5 of Annex III placed on the market or put into service by financial institutions that are subject to requirements under Union financial services law regarding their internal governance, arrangements or processes

VALUE CHAIN AND OBLIGATIONS OF DISTRIBUTORS, IMPORTERS, DEPLOYERS OR OTHER THIRD-PARTIES

Art. 25(3):

For high-risk AI systems as safety components of products subject to EU 'New Approach' harmonisation rules, the product manufacturer shall be considered to be the provider of the high-risk system and shall be subject to the obligations under Article 16 under either of the following circumstances:

- the high-risk AI system is placed on the market together with the product under the product manufacturer's name or trademark;
- the high-risk AI system is put into service under the product manufacturer's name or trademark after the product has been placed on the market.

Co-funded by the Erasmus+ Programme of the European Union

VALUE CHAIN AND OPERATORS' OBLIGATIONS

Conformity assessment and European standards (Art. 40-49)

Compliance of a high-risk AI system with mandatory requirements is presumed if the provider applies harmonised standards established by European standardisation organisations or, in the absence of such standards and until their adoption, common specifications established by the Commission

- For products subject to EU ‘new approach’ standards: relevant conformity assessment procedure;
- For Annex III AI systems (except those used for biometrics): internal control (the Commission may, by means of delegated acts, impose the use of notified bodies).

Notified bodies issue certificates valid for 4 years (5 for products). The provider completes an EU declaration of conformity attesting that the mandatory requirements have been met and by which he assumes responsibility for conformity.

For exceptional reasons of protection of important public interests (security, health, etc.), or in the case of specific, substantial and imminent threat to the life or physical safety of natural persons, law-enforcement authorities or civil protection authorities may authorise the marketing of high-risk AI systems without a conformity assessment procedure (with Commission supervision).

Co-funded by the Erasmus+ Programme of the European Union

VALUE CHAIN AND OPERATORS' OBLIGATIONS

Importer (Art. 3(6)): A natural or legal person located or established in the Union that places on the market an AI system that bears the name or trademark of a natural or legal person established in a third country.

Obligations on importers of high-risk AI systems (Art. 23):

- before placing the system on the market, the importer must verify its conformity (1. conformity assessment procedure referred to in Art. 43; 2. technical documentation in accordance with Art. 11; 3. CE marking and EU declaration of conformity referred to in Art. 47; 4. appointment of an authorised representative).
- the importer must refrain from placing on the market systems deemed non-compliant/falsified or accompanied by falsified documentation; in the event of a risk, inform the provider and the supervisory authorities;
- the impoert must indicate their references on the packaging/accompanying document; ensure that transport/storage conditions do not jeopardise compliance;
- the importer must keep documentation; cooperate with competent authorities.

VALUE CHAIN AND OPERATORS' OBLIGATIONS

Distributor (Art. 3(7)): a natural or legal person in the supply chain, other than the provider or the importer, that makes an AI system available on the Union market.

Obligations on distributors of high-risk AI systems (Art. 24):

- before making the high-risk AI system available on the market, distributors must verify the presence of the required (1) CE marking, (2) copy of the EU declaration of conformity and (3) instructions for use;
- refrain from making a system available on the market that is considered non-compliant;
- inform the provider/importer of any risks;
- ensure that storage/transport conditions do not jeopardise the compliance of the system;
- if they consider that a system already made available on the market does not comply with the requirements, take the necessary corrective measures, or withdraw/recall the system; if the system presents a risk, inform the provider/importer and the authorities and cooperate with them.

VALUE CHAIN AND OPERATORS' OBLIGATIONS

Deployer (Art. 3(4); recital 13): a 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.

They are subject to the AI Act (Art. 2(1) b-c):

- deployers of AI systems that have their place of establishment or are located within the Union;
- providers and deployers of AI systems that have their place of establishment or are located in a third country, where the output produced by the AI system is used in the Union.

VALUE CHAIN AND OPERATORS' OBLIGATIONS

In certain circumstances, the deployer (as well as the distributor, importer or other third party) is considered to be the provider of a high-risk AI system and assumes the corresponding obligations (Art. 25; recital 84):

(a) if it affixes its name or trademark to a high-risk AI system that has already been placed on the market or put into service (without prejudice to contractual agreements providing for a different division of obligations);

(b) if it makes a substantial change to a high-risk AI system already placed on the market or put into service so that it remains high-risk;

(c) if it changes the intended purpose of an AI system (including GPAIs) not classified as high risk so that it becomes high risk.

In such cases, the initial provider must cooperate closely with the new providers (information, reasonably expected technical access and any other assistance), unless it has clearly excluded the transformation of its system into a high-risk AI system.

VALUE CHAIN AND OPERATORS' OBLIGATIONS

Obligations on deployers of high-risk AI systems (Art. 26; recitals 91-95)

- take appropriate technical and organisational measures to ensure that high-risk AI systems are used in accordance with the instructions for use;
- entrust human supervision to natural persons who have the necessary competence, training and authority;
- ensure that input data (if under its control) are relevant and sufficiently representative in light of the intended purpose of the system;
- monitor the operation of the system in accordance with the instructions for use (transmitting the relevant information to the provider). If they consider that the use of the system may present a risk, they inform the provider/distributor and the supervisory authority without delay and suspend the use of the system. If they detect a serious incident, they inform the provider/importer/distributor and the supervisory authority.
- keep the logs automatically generated by the system for a period appropriate to the intended purpose of the system (not less than six months);
- if the deployer is an employer and the system is intended to be used in the workplace, inform workers' representatives and the workers concerned;
- for remote biometric identification systems to be used for the targeted search of a suspected or convicted offender, request prior judicial or administrative authorisation within 48 hours;
- for systems listed in Annex III that take decisions or assist in taking decisions concerning natural persons, inform them that they are subject to the use of the high-risk system;
- cooperate with the competent authorities.

Co-funded by the Erasmus+ Programme of the European Union

VALUE CHAIN AND OPERATORS' OBLIGATIONS

Obligations for deployers of high-risk AI systems (Art. 27; recital 96)

- Deployers of Annex III systems (except those related to critical infrastructure security) that are public law bodies or private entities providing public services or entities that use credit scoring or risk assessment/pricing systems for life and health insurance: prior to first use of the system, they shall perform an assessment of the impact on fundamental rights that the use of such system may produce. Once the assessment has been performed, the deployer shall notify the market surveillance authority of its results, submitting the filled-out template referred to in paragraph 5 of Article 27 as part of the notification. In the case referred to in Article 46(1), deployers may be exempt from that obligation to notify.

The template includes (1) a description of the deployer's processes in which the system will be used according to its intended purpose; (2) period of time/frequency of use; (3) categories of natural persons and groups affected by the use and their specific risks of harm; (4) specific risks of harm likely to have an impact on the categories of natural persons or groups of persons; (5) human oversight measures implemented; (6) measures to be taken if risks materialise, including internal governance arrangements and grievance mechanisms.

VALUE CHAIN AND OPERATORS' OBLIGATIONS

Obligations on deployers of high-risk AI systems (Art. 86; recital 171)

Every data subject who is the subject of a decision taken by the deployer on the basis of the output of a high-risk AI system referred to in Annex III and which produces legal effects or similarly significantly affects him/her in a way that he/she considers to have an adverse impact on his/her health/safety/basic rights shall have the right to obtain clear and meaningful explanations from the deployer on the role of the AI system in the decision-making process and on the main elements of the decision taken.

VALUE CHAIN AND OPERATORS' OBLIGATIONS

Obligations on third parties providing elements of a high-risk AI system (Art. 25.4; recitals 88-90)

- Third parties that provide AI systems, tools, services, components or processes used or integrated into a high-risk AI system are required to provide the provider of the high-risk system, by written agreement, with the information, capabilities, technical access and any other assistance necessary to enable the provider to fully perform its obligations.

- Third parties who make tools, services, processes or components, other than GPAIs, publicly available under a free and open source licence are excluded.

- Voluntary standard contractual clauses will be developed by the AI Office, which will take into account the possible contractual requirements applicable in certain sectors and business cases.

VALUE CHAIN AND OPERATORS' OBLIGATIONS

Providers of certain AI systems (Art. 50(1-2); recitals 132-133) regardless of whether they are considered high-risk or not

- Providers of AI systems intended to interact directly with natural persons must design and develop the system in such a way that persons are informed (notified) that they are interacting with an AI system, unless this would not be apparent to a reasonably informed, observant and circumspect person, taking into account the circumstances and context of use (e.g., interaction with persons vulnerable by age or disability).

- Providers of AI systems, including GPAIs, that generate audio, image, video or synthetic text content, must be marked in a machine-readable format (watermarks, cryptographic methods, etc.) and detectable as artificially generated or manipulated.

- Exception for AI systems with a standard editing assistance function or which do not substantially alter the input data provided by the deployer or the respective semantics.

VALUE CHAIN AND OPERATORS' OBLIGATIONS

Deployer of certain AI systems (Art. 50(3)-(4); recital 132-134) regardless of whether they are considered high-risk or not

- Deployers of emotion-recognition or biometric categorisation systems must inform exposed natural persons about the operation of the system and complying with data protection regulations.

- Deployers of AI systems that generate or manipulate images or audio or video content that constitutes a deep fake must disclose that the content has been artificially generated or manipulated (if such content is part of a manifestly artistic or creative work or programme, etc., disclose the existence of the generated/manipulated content without hindering the exhibition or enjoyment of the work).

- Deployers of AI systems that generate/manipulate published text for the purpose of informing the public about matters of public interest must disclose that the text has been artificially generated/manipulated (exception for content subject to human review or control by an editorial manager).

OBLIGATIONS FOR GPAI MODELS PROVIDERS (ART. 53-56)

- draw up and keep up-to-date technical documentation of the model, including the training and testing process and the results of its evaluation (see minimum elements in Annex XI, including known or estimated energy consumption), to be forwarded on request to the AI Office and the competent national authorities.

- prepare and make available information and documentation to downstream providers that intend to integrate the GPAI model into their AI system, enabling them to have a good understanding of the capabilities and limitations of the GPAI model and to fulfil their obligations (see minimum elements in Annex XII).

- implement a policy of compliance with the EU copyright rules (including conditions of operation of the 'text and data mining' exception).

- draft and publish a detailed summary of training content.

- if established in third countries, appoint an authorised representative.

Co-funded by the Erasmus+ Programme of the European Union

OBLIGATIONS ON GPAIS MODEL PROVIDERS (ARTS. 53-56)

- Providers of GPAI models released under a free and open source licence (which can be freely accessed, used, modified and distributed) are exempted from the technical documentation/information requirements to downstream providers provided that the relevant parameters, including weights, information on model architecture and information on model use, are made public (the exception does not apply to GPAI models with systemic risk).

- Providers of GPAI models with systemic risk are subject to additional obligations: (1) perform an assessment of the models in accordance with standardised protocols and tools; to assess and mitigate possible systemic risks; (2) assess and mitigate possible systemic risks at Union level, including their sources, that may stem from the development, the placing on the market, or the use of GPAI models with systemic risk; (3) track document and report serious incidents and possible corrective measures to the AI Office and relevant national authorities; (4) ensure an adequate level of cybersecurity protection.

- Codes of good practice are envisaged (driving and monitoring role of the AI Office), to which the Commission may give general validity; failing this, the Commission will define common standards.

GOVERNANCE AND ENFORCEMENT: EU LEVEL (Artt. 56, 64, 75, 95; recital 116, 148, 161, 162, 164)

- The AI Office, within the administrative structure of DG CNECT (Decision C(2024) 390), works to support the Commission in the implementation of the AI Act, with specific tasks related mainly to GPAIs, including the development of tools, methodologies and benchmarks for assessing the capacity of GPAI models, in particular those with systemic risks, monitoring their functioning and the emergence of unforeseen risks, and conducting investigations into possible breaches of the rules.

- The AI Office also assists the Commission in the preparation of decisions, executive and delegated acts, guidelines, requests for standardisation and definition of common specifications, coordinates the establishment of the governance system for the application of the regulation, and promotes the adoption of codes of conduct at EU level (GPAIs, marking obligations for artificially generated or manipulated content). In implementing its tasks, the AI Office is called upon to ensure cooperation with stakeholders, through consultations and ad hoc fora.

GOVERNANCE AND ENFORCEMENT: EU LEVEL

- The European Artificial Intelligence Board (Art. 65 and 66), composed of one representative per Member State, provides advice and assistance to the Commission and the Member States to facilitate the consistent and effective implementation of the regulation (collection and sharing of best technical and regulatory practices, contribution to the harmonisation of administrative practices, recommendations and opinions on relevant issues, including evolving trends in AI value chains, support for Commission initiatives on literacy, etc.).

- An Advisory Forum (Art. 67), composed of stakeholder representatives, provides advice and technical expertise to the European Artificial Intelligence Board and the Commission.

- A Scientific panel of independent experts (Art. 68) selected by the Commission provides advice and support to the Office of AI for the implementation of the regulation, in particular with regard to the supervision of GPAI systems and models and cross-border investigative activities (if serious risks in two or more Member States).

GOVERNANCE AND ENFORCEMENT: NATIONAL LEVEL

Member States shall designate at least one notifying authority and one market surveillance authority (Art. 70) which:

- exercise their powers independently, impartially and without bias;
- have adequate technical, financial and human resources (sufficient staff to ensure in-depth understanding of AI technologies, data and computing, personal data protection, cybersecurity, fundamental rights, health and safety risks, and knowledge of existing standards and legal requirements), as well as the infrastructure needed to perform their tasks effectively;
- may provide advice and guidance on the implementation of the regulation, in particular to SMEs including start-ups; when ruling on AI systems in areas covered by EU regulations, they consult the relevant sectoral authorities at national level.

A market surveillance authority is designated as single point of contact.

GOVERNANCE AND ENFORCEMENT: NATIONAL LEVEL

The notifying authority is responsible for the notification procedures and subsequent monitoring of conformity assessment bodies for high-risk AI systems (Art. 28-39).

- once it receives the application from the body concerned, it verifies the requirements laid down in the regulation, relating to the independence of the body (as well as any subcontractors or subsidiaries) from providers of the systems subject to conformity assessment and their competitors, and to internal organisation and management measures, which must guarantee the impartiality of assessment activities and the protection of confidentiality of information.

- notifies the Commission and the other Member States (which may raise objections within a given period of time) of the bodies deemed to fulfil the requirements, which are placed on a public list.

- limits, suspends or withdraws the designation of a notified body that no longer meets the requirements or fails to fulfil its obligations (of information on certificates issued and subsequent events).

GOVERNANCE AND ENFORCEMENT: NATIONAL LEVEL

For specific areas, the market surveillance authority's choice is constrained:

- for high-risk AI systems linked to products subject to the Union harmonisation legislation, it is the one designated under the relevant legislation (Art. 74(3));
- for high-risk AI systems directly linked to the provision of financial services regulated by EU law, it is the one responsible for the financial supervision of the institutions that market/service/use the AI system (Art. 74(6));
- for some of the high-risk AI systems listed in Annex III (biometrics; law enforcement; migration/asylum/border control; administration of justice and democratic processes), Member States designate as market surveillance authorities the competent data protection authorities under the GDPR or Dir. (EU) 2016/680 (Art. 70(8));

Outside of these areas, Member States enjoy autonomy in their choice.

Co-funded by the Erasmus+ Programme of the European Union

GOVERNANCE AND ENFORCEMENT: NATIONAL LEVEL

Market surveillance authorities operate according to the procedures and powers governed by Regulation (EU) 2019/1020 on market surveillance and conformity of products (Art. 74(1)). In order to perform their tasks, they have full access to the training, validation and test documentation and datasets used for the development of high-risk AI systems and, upon reasoned request, under certain conditions can access the source code (Art. 74(12)-(13)).

In the event of serious incidents, upon receipt of a report from the provider of the high-risk AI system, the market surveillance authorities inform the national authorities protecting fundamental rights, take appropriate measures (withdrawal, recall) and follows the notification procedures laid down in Reg. (EU) 2019/1010: Rapex rapid information system to the Commission (Art. 73).

Market surveillance authorities authorise and monitor the conduct of tests of AI systems under real conditions (both inside and outside sandboxes) and take any measures to modify, suspend or terminate the tests (Art. 60, 76).

Market surveillance authorities receive complaints about alleged breaches of the rules (Art. 85); whistleblowers benefit from whistleblower protection (Art. 87).

GOVERNANCE AND ENFORCEMENT: NATIONAL LEVEL

The market surveillance authority, in its market control/monitoring activities, may find that (Art. 79-83):

- an AI system poses a risk the market surveillance authority carries out an assessment of compliance of the AI system with the requirements/obligations of the regulation.

In the event of non-compliance, the market surveillance authority asks the operator concerned to take appropriate corrective action/withdraw/revocate the system from the market. If the operator fails to comply, the market surveillance authority takes provisional restrictive measures and notifies them to the Commission and the other Member States for possible objections. If no objections are raised, the measure is deemed justified and similar restrictive measures are taken in all Member States concerned.

If the market surveillance authority considers that, although compliant with the Regulation, a high-risk AI system nevertheless presents a risk, it requires the operator concerned to take appropriate measures to eliminate it and informs the Commission and the other Member States accordingly. The Commission decides whether the measure is justified and proposes any other appropriate measures.

GOVERNANCE AND ENFORCEMENT: NATIONAL LEVEL

- An AI system classified by the provider as not high risk under Art. 6(3) is in fact high riskà at the outcome of the assessment, the market surveillance authority shall require the provider to bring the system into compliance with the requirements and obligations of the Regulation, as well as to take appropriate corrective measures, and shall inform the Commission and the other Member States. The non-compliant provider shall be subject to financial penalties. The market surveillance authority adopts provisional restrictive measures, which may be objected to by the Commission or the other Member States; in the absence of objections, the measures are deemed justified and similar restrictive measures are adopted in the other Member States concerned.

- Safeguard procedure: if the Commission or other market surveillance authorities object to restrictive measures taken at national level (within 3 months/30 days for non-compliance with Article 5 prohibitions), the Commission decides whether the measure is justified. If so, all states take restrictive measures; if not, the measure must be withdrawn.

- If formal defects are present (absence of CE marking or EU declaration of conformity, etc.), the market surveillance authority takes restrictive measures if the provider does not remedy them.

SUPERVISION ON GPAIs

The Commission has exclusive competence and exercises it through the AI Office, which investigates possible breaches of the rules, either on its own initiative, based on its monitoring activities, or at the request of market surveillance authorities.

The AI Office:

- receives complaints from downstream providers concerning breaches of the regulation by GPAI model providers as well as reports from the Panel (concerning alleged concrete and identifiable risks at EU level or the classification of GPAI models as ‘systemic risk’) (Art. 89).
- may request documentation and information from the GPAI models provider (Art. 91).
- after consulting the European Artificial Intelligence Board, may conduct assessments of the GPAI to (1) assess compliance with obligations and (2) investigate systemic risks at EU level, including by requesting access to the GPAI in question (Art. 92).
- may require the adoption of measures (compliance/restrictive/systemic risk mitigation) by the GPAI provider.

COOPERATION MECHANISMS BETWEEN EU AND NATIONAL LEVELS

Member States are required to facilitate the tasks of the AI Office (Art. 64(1)) and to inform it of sandboxes and results (Art. 57(15)).

Notifying authorities notify the Commission and the other Member States of conformity assessment bodies and relevant changes to the notification (Artt. 30, 36). They inform the Commission and the other Member States of authorisations derogating from the conformity assessment procedure (Art. 46). In both cases, verification procedures at European level.

In the event of a serious incident, market surveillance authorities notify the measures taken through RAPEX (Art. 73(9)). They may propose joint activities/investigations with the Commission on categories of high-risk AI systems that present a serious risk in two or more Member States (Art. 74(2)). If they consider that high-risk AI systems are not in compliance with the RAPEX system, they may propose joint activities/investigations with the Commission on categories of high-risk AI systems that present a serious risk in two or more Member States (Art. 74(3)). 11). If they consider that GPAI systems that can be used directly by deployers for at least one high-risk purpose do not comply with the requirements of the Regulation, they cooperate with the AI Office to carry out compliance assessments and may request the AI Office for access to information on the AI model needed to conclude investigations on a high-risk AI system (Art. 75(2)-(3)).

PENALTIES

Artt. 99, 101

Member States shall lay down the rules on sanctions ('effective, proportionate and dissuasive') and other enforcement measures.

- Violation of Article 5 prohibitions: up to € 35 milions or 7% of worldwide turnover, whichever is higher.
- Violation of requirements for high risk AI systems and transparency obligations under Art. 50: up to € 15 millions or 3% total worldwide turnover whichever is higher.
- Provision of incorrect, incomplete or misleading information to notified bodies or competent authorities: up to € 7.5 millions or 1% total worldwide turnover, whichever is greater.
- Infringements committed by GPAI models providers (including failure to comply with requests for documents/information and failure to grant the Commission access to the model): up to 3% of total worldwide turnover or EUR 15 millions, whichever is higher. Penalties are imposed by the Commission. Judicial reviews are carried out by the Court of Justice.

AI REGULATORY SANDBOXES

Art. 57

Member States (including jointly) establish regulatory sandboxes for AI, providing a controlled environment (under the guidance of the competent authorities) that facilitates the development, training, testing and validation of innovative AI systems for a period of time prior to their placing on the market/commissioning; within the sandboxes, personal data may be processed under certain conditions and with appropriate measures.

The competent authorities may suspend the testing process if significant risks emerge that cannot be mitigated with appropriate measures. Providers and potential providers participating in sandboxes remain liable for damages to third parties but, if they have complied with the plan and terms of participation and followed the guidelines of the competent authorities, they are exempt from penalties.

The functioning of sandboxes will be defined by Commission implementing acts so as to ensure broad and equal access, flexibility, free of charge for SMEs, etc.

ENTRY INTO FORCE AND APPLICATION

The AI Act will enter into force 20 days after its publication in the Official Journal of the EU and will start to apply 24 months after its entry into force, except for:

- the prohibitions on prohibited practices, which will apply 6 months after entry into force;
- the codes of good practice (9 months after);
- the rules on AI systems for general purposes, including governance (12 months);
- the obligations for high-risk systems (36 months).

Without prejudice to the application of the prohibitions, exemptions and adaptation periods (3-6 years) are provided for GPAIs/high-risk AI systems placed on the market/commissioned before 12 months after entry into force).

IMPACT OF THE AI ACT ON THE ECOSYSTEM

GREATER RELIANCE ON AI	Increased adoption of AI by citizens and consumers
ALLOCATION OF RESOURCES	High investment needed by the public sector
REGULATORY BURDEN	High compliance costs and bureaucracy

The case of the AI Act

To sum up…

Objectives of the AI Act

The proposed regulatory framework on Artificial Intelligence has the following objectives:

1. ensure that AI systems placed on the Union market and used are safe and respect existing law on fundamental rights and Union values;

2. ensure legal certainty to facilitate investment and innovation in AI;

3. enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems;

4. facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation.

Subject Matter of the AI Act

The scope of the AI Act is largely determined by the subject matter to which the rules apply. In that regard, Article 1 states that:

Article 1

Subject matter

This Regulation lays down:

(a) harmonised rules for the placing on the market, the putting into service and the use of artificial intelligence systems (‘AI systems’) in the Union;

(a) prohibitions of certain artificial intelligence practices;

(b) specific requirements for high-risk AI systems and obligations for operators of such systems;

(c) harmonised transparency rules for AI systems intended to interact with natural persons, emotion recognition systems and biometric categorisation systems, and AI systems used to generate or manipulate image, audio or video content;

(d) rules on market monitoring and surveillance.

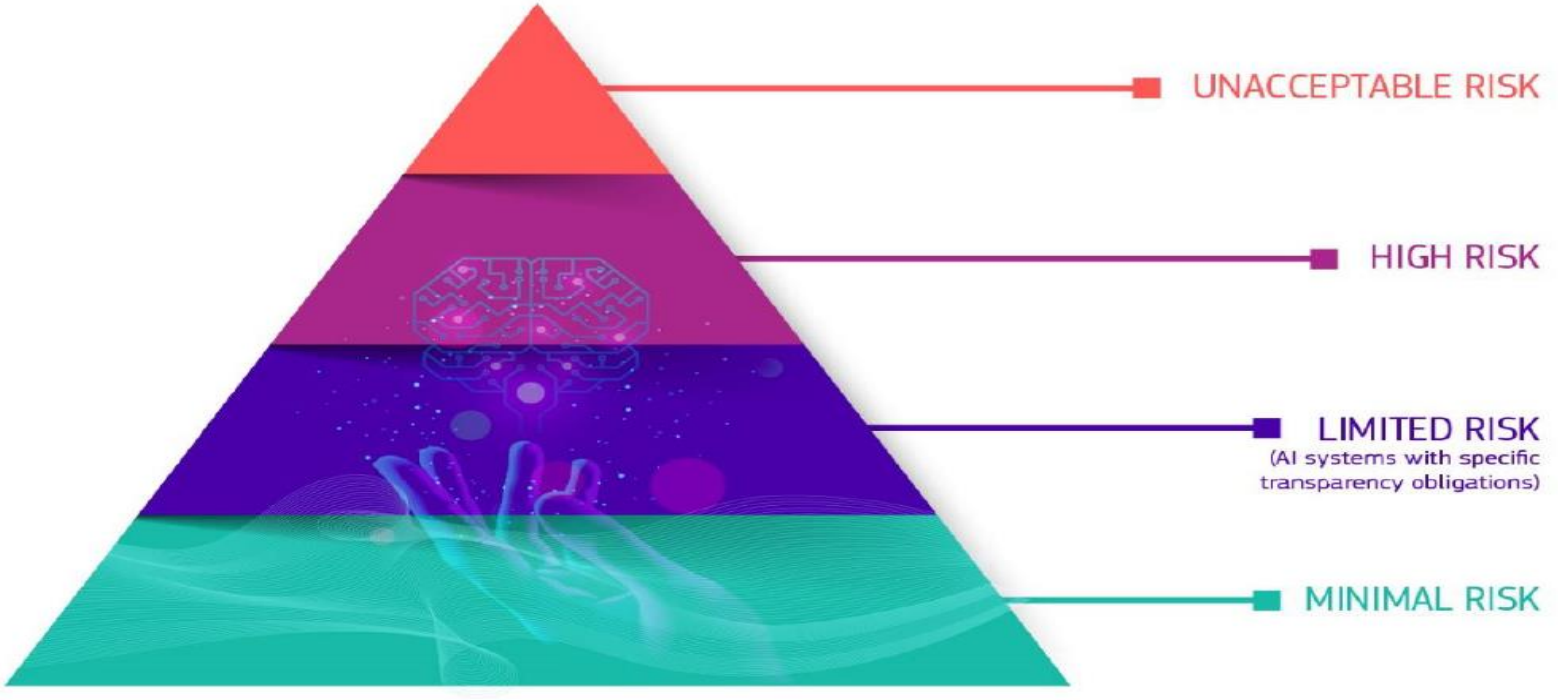
Pyramid of Criticality: Risk based approach

To achieve the goals outlined, the Artificial Intelligence Act draft combines a risk-based approach based on the pyramid of criticality, with a modern, layered enforcement mechanism.

This means, among other things, that a lighter legal regime applies to AI applications with a negligible risk, and that applications with an unacceptable risk are banned.

Between these extremes of the spectrum, stricter regulations apply as risk increases. These range from non-binding self-regulatory soft law impact assessments accompanied by codes of conduct, to heavy, externally audited compliance requirements throughout the life cycle of the application.

Pyramid of Criticality: Risk based approach



The Pyramid of Criticality for AI Systems

Unacceptable Risk AI systems

Unacceptable Risk AI systems can be divided into 4 categories: two of these concern cognitive behavioral manipulation of persons or specific vulnerable groups. The other 2 prohibited categories are social scoring and real-time and remote biometric identification systems. There are, however, exceptions to the main rule for each category. The criterion for qualification as an Unacceptable Risk AI system is the harm requirement.

Examples of High-Risk AI-Systems

Hi-Risk AI-systems will be carefully assessed before being put on the market and throughout their lifecycle. Some examples include:

- Critical infrastructures (e.g. transport), that could put the life and health of citizens at risk
- Educational or vocational training, that may determine the access to education and professional course of someone's life (e.g. scoring of exams)
- Safety components of products (e.g. AI application in robot-assisted surgery)

Unacceptable Risk AI systems

Unacceptable Risk AI systems

- Employment, workers management and access to self-employment (e.g. CV sorting software for recruitment procedures)
- Essential private and public services (e.g. credit scoring denying citizens opportunity to obtain a loan)
- Law enforcement that may interfere with people's fundamental rights (e.g. evaluation of the reliability of evidence)
- Migration, asylum and border control management (e.g. verification of authenticity of travel documents)
- Administration of justice and democratic processes (e.g. applying the law to a concrete set of facts)
- Surveillance systems (e.g. biometric monitoring for law enforcement, facial recognition systems)

Market Entrance of High-Risk AI-Systems: 4 Steps

- In a nutshell, these 4 steps should be followed prior to Hi-Risk AI-Systems market entrance. Note that these steps apply to components of such AI systems as well.

1. A High-Risk AI system is developed, preferably using internal ex ante AI Impact Assessments and Codes of Conduct overseen by inclusive, multidisciplinary teams.
2. The High-Risk AI system must undergo an approved conformity assessment and continuously comply with AI requirements as set forth in the EU AI Act, during its lifecycle. For certain systems an external notified body will be involved in the conformity assessment audit. This dynamic process ensures benchmarking, monitoring and validation. Moreover, in case of changes to the High-Risk AI system, step 2 has to be repeated.

3. Registration of the stand-alone Hi-Risk AI system will take place in a dedicated EU database.

4. A declaration of conformity must be signed and the Hi-Risk AI system must carry the CE marking (Conformité Européenne). Now the system is ready to enter the European markets.

Market Entrance of High-Risk AI-Systems: 4 Steps

But this is not the end of the story...

In the vision of the EC, after the Hi-Risk AI system haven obtained market approval, authorities on both Union and Member State level 'will be responsible for market surveillance, end users ensure monitoring and human oversight, while providers have a post-market monitoring system in place.

Providers and users will also report serious incidents and malfunctioning. In other words, continuous upstream and downstream monitoring.

Since people have the right to know if and when they are interacting with a machine's algorithm instead of a human being, the AI Act introduces specific transparency obligations for both users and providers of AI system, such as bot disclosure. Likewise, specific transparency obligations apply to automated emotion recognition systems, biometric categorization and deepfake/synthetics disclosure. Limited Risk AI Systems such as chatbots necessitate specific transparency obligations as well. The only category exempt from these transparency obligations can be found at the bottom of the pyramid of criticality: the Minimal Risk AI Systems.

In addition, natural persons should be able to oversee the Hi-Risk AI-System. This is termed the human oversight requirement.

Open Norms

The definition of high-risk AI applications is not yet set in stone. Article 6 does provide classification rules. Presumably, the qualification remains a somewhat open standard within the regulation, subject to changing societal views, and to be interpreted by the courts, ultimately by the EU Court of Justice. A standard that is open in terms of content and that needs to be fleshed out in more detail under different circumstances, for example using a catalog of viewpoints. Open standards entail the risk of differences of opinion about their interpretation. If the legislator does not offer sufficient guidance, the courts will ultimately have to make a decision about the interpretation of a standard.

This can be seen as a less desirable side of regulating with open standards. A clear risk taxonomy will contribute to legal certainty and offer stakeholders with appropriate answers to questions about liability and insurance.

Enforcement

The AI Act provides for the installation of a new enforcement body at Union level: the European Artificial Intelligence Board (AI Board). At Member State level, the AI Board will be flanked by national supervisors, similar to the GDPR's oversight mechanism. Fines for violation of the rules can be up to 6% of global turnover, or 30 million euros for private entities.

'The proposed rules will be enforced through a governance system at Member States level, building on already existing structures, and a cooperation mechanism at Union level with the establishment of a European Artificial Intelligence Board.'

AI Office

The Commission has established a new EU level regulator, the European AI Office, which will sit within the Directorate-General for Communication Networks, Content and Technology (DG CNECT) in the Commission.

The AI Office will monitor, supervise, and enforce the AI Act requirements on general purpose AI (GPAI) models and systems across the 27 EU Member States. This includes analysing emerging unforeseen systemic risks stemming from GPAI development and deployment, as well as developing capabilities evaluations, conducting model evaluations and investigating incidents of potential infringement and non-compliance. To facilitate the compliance of GPAI model providers and consider their perspectives, the AI Office will produce voluntary codes of practice, adherence to which would create a presumption of conformity.

The AI Office will also lead the EU in international cooperation on AI and strengthen bonds between the European Commission and the scientific community, including the forthcoming scientific panel of independent experts. The Office will help the 27 Member States cooperate on enforcement, including on joint investigations, and act as the Secretariat of the AI Board, the intergovernmental forum for coordination between national regulators. It will support the creation of regulatory sandboxes where companies can test AI systems in a controlled environment. It will also provide information and resources to small and medium businesses (SMEs) to aid in their compliance with rules

Università Europea di Roma

Co-funded by the Erasmus+ Programme of the European Union

AI & FUNDAMENTAL RIGHTS

AI & Fundamental Rights

Fundamental rights are mentioned throughout the AI Act as an overriding public interest that warrants legislative protection.

In particular, Article 65(1) AI Act extends the definition of product risks to include risks to fundamental rights. The result is a product safety instrument heavily couched in fundamental rights language.

The AI Act is not the first product safety instrument to cover fundamental rights.

AI & Fundamental rights

The EU regulation that lays down harmonized rules for medical devices (Medical Devices Regulation: Regulation (EU) 2017/745) explicitly refers to the protection of fundamental rights in general (Recital 89) and personal data more specifically (Recital 69) while including extra safeguards to two specific freedoms: freedom of expression and freedom of the press.

More generally, the EU is constitutionally required to protect fundamental rights as it exercises its powers, including in product safety.

AI & Fundamental Rights

However, the AI Act **displays a higher level of engagement with fundamental rights than other EU product safety instruments**. This can be seen in the practical requirements imposed on AI systems.

The segmentation of AI systems into various risk tiers **puts risks to fundamental rights on an equal footing with the risks to health and safety that are the bread and butter of product safety law.** Various essential requirements laid down for high-risk AI systems are formulated in terms of fundamental rights, such as the need to indicate circumstances in which the use of the AI system may impose risks or to design suitable mechanisms for human oversight of the AI system. Finally, conformity with essential requirements must be assessed, considering how well an AI system minimizes or eliminates risks to fundamental rights.

AI & Fundamental Rights

: Comparison between rationales in product safety law and constitutional reasoning

Product safety	Fundamental rights
Actuarial risks predominate	Actuarial, sociopolitical, and cultural risks
Risks stem from the technical object	Risks stem from the sociotechnical context
Small world: known and consistent problems	Multidimensional harm and wicked problems
Satisficing technical baselines	Constrained maximization of principles

Fundamental Rights' concerns

In 2019, the EU's High-Level Expert Group (HLEG) on AI published an **updated definition of AI, including its main capabilities and scientific disciplines** (High-Level Expert Group on Artificial Intelligence (HLEG), A Definition of AI: Main Capabilities and Disciplines, ec.europa.eu, p. 6).

According to this definition, AI systems **are designed by humans but can come in different forms, such as machine learning, machine reasoning, and robotics**.

Fundamental Rights' concerns

In all its forms but to varying degrees, AI is currently capable of acquiring, processing, and interpreting large amounts of data, making decisions based on the interpreted data, and translating these decisions into action.

Based on what AI is capable of, four specific characteristics become visible which, however, **do not only come with benefits but may also lead to fundamental rights concerns**.

Privacy concerns & deanonymization

First, AI is dependent on data, hence, it has enhanced capacities to collect and process large amounts of data. This gives AI an **increased power of human observation, for example, through biometric identification in public places, thus raising privacy concerns**.

Secondly, through the connectivity of many AI systems and by analyzing large amounts of data and identifying links among them, **AI may be used to deanonymise large data sets although such data** sets do not include personal data *per se*.

Black-box scenario & discrimination

Thirdly, based on the self-learning ability of AI and, hence, its increasing autonomy, coupled with the enhanced capacity of AI to learn quickly and explore decision paths that humans might not have thought about, AI is able to **find patterns of correlation within datasets without necessarily making a statement on causation**. Consequently, AI may produce new solutions that may be impossible for humans to grasp by making decisions without the reasons being known, potentially resulting in AI opaqueness. This opaqueness is **also known as the 'black-box phenomenon'** which drastically reduces the explainability of AI.

Fourthly, the training data of AI systems may be biased, leading to **AI systems producing discriminatory results**.

Fundamental Rights protection and EU Treaties

The EU Treaties provide for a **general guarantee of fundamental rights** protection.

Nonetheless, general principles of EU law have been constituting the principal source of fundamental rights protection in the EU whereby the **Charter of Fundamental Rights of the EU (the Charter) now codifies these fundamental rights**.

Specifically, **Arts 7, 8, and 21 lay down the rights to privacy, protection of personal data, and non-discrimination, respectively**. The European Commission has expressed **concerns regarding the limited scope of application of the EU Charter in the context of the AI discussion** (European Commission, Structure for the White Paper on artificial intelligence – a European approach).

AI systems and Charter scope of application

According to Art. 51 of the Charter and the case law of the CJEU, the Charter and general principles of EU law **apply to any action falling within the scope of EU law**.

Consequently, certain Member States' actions involving the development and/or use of AI systems may not fall within the Charter's field of application and may, thus, potentially lead to a compromised fundamental rights protection. For example, the **use of AI systems in the industry or the health sector is only partially or not covered at all by the Charter's scope of application because these fields fall primarily within the exclusive competences of the Member States**.

AI systems and Charter scope of application

Nevertheless, the EU often takes on an active supportive role to protect fundamental rights by adopting guidelines, even in areas that fall outside its main competences. For example, in the health sector, the Commission has adopted guidelines for Member States on the Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) app, designed to help tackle the Covid-19 crisis by tracing infection chains, even across borders. The app is largely based on advanced algorithms and, hence, touches upon privacy and data protection concerns of interest by the Union.

AI systems and Charter scope of application

Another concern that was raised by the Commission was the **lack of horizontal direct effect of the Charter**. However, it must be noted that the Court has practically acknowledged the direct horizontal application of the Charter in specific situations, namely when EU secondary law gives expression to a general principle of EU law, such as the principles of privacy and protection of personal data and non-discrimination.

Hence, the use of AI systems must be in conformity with these principles, even in horizontal situations falling within the scope of EU law. For example, the observance of the principle of non-discrimination in situations covered by Directive 2000/78/EC on equal treatment in employment and occupation is particularly important when AI systems are used for recruitment purposes in employment matters, amongst others.

Fundamental Rights and GDPR

The GDPR is, amongst others, **specifically intended to apply to partly or fully automatic AI systems that process personal data forming part or intended to form part of a filing system**.

At the same time, the use of AI systems is limited under the GDPR. For example, while the GDPR applies to the processing of personal data by wholly automated means, Art. 22, para. 1, prohibits the use of fully autonomous AI systems for the processing of personal data which produces legal effects for individuals.

Hence, the GDPR limits the development and use of AI to systems that still function with some sort of meaningful human oversight.

Fundamental Rights and GDPR

Additionally, also functioning as one exception to the prohibition laid down in Art. 22, para. 1, the processing of personal data can only take place based on the specific consent of the data subject. The concept of specific consent entails informed consent, meaning that the **data subject must not only be informed that her personal data is being processed but also about how and for what purposes the processing takes place**.

While, in theory, the requirement of consent should provide for sufficient safeguards against fundamental rights violations by AI systems processing personal data, **it is difficult to obtain informed consent when AI systems make unpredictable decisions**.

Fundamental Rights and GDPR (AI and consent)

Moreover, the means of obtaining the specific consent of the data subject, such as “I have read and agree to the Terms”, is one of the biggest lies on the internet that poses the risk of rendering the protection offered by the concept of specific consent inefficient. To avoid this, it can be assumed that the use of fully, as well as partly automated AI systems, is further limited by the principle of controller responsibility under the GDPR.

For example, in Google Spain, the CJEU found that a search engine operator is a controller within the meaning of Art. 4, para. 7, GDPR when she processes personal data. This is when the activity of the search engine consists of finding information, indexing it automatically, storing it temporarily, and making it available to internet users, when that information consists of personal data. If this is the case, the controller has a responsibility to, under specific circumstances, remove searches based on a person’s name from the list of results. Although certain of these processing procedures by a search engine may be done by AI systems, it is the search engine operator who has the ultimate responsibility, thus limiting the use of AI systems in such circumstances.

Fundamental Rights and GDPR

Moreover, in GC and Others v. CNIL, the Court held that it is the responsibility of a search engine operator, when receiving a de-referencing request, to balance the right to personal data protection against other rights which may be affected by the de-referencing, for example, the right to freedom of information. Hence again, the use of AI systems for the operation of search engines is limited by the operator's responsibility to oversee and guarantee the necessary fundamental rights protection. In conclusion, this means that the full potential of AI can never be used in situations falling under the GDPR.

Considering this in the light of fundamental rights, the development and use of AI systems are generally limited by the concepts of specific consent and controller responsibility to safeguard the protection of the rights of the data subjects.

Fundamental Rights and GDPR (transparency and explainability)

As regards the opacity in AI decision-making, the GDPR requires the observance of the principles of transparency and explainability, including the data subject's rights to information and access to personal data. To uphold these principles, this also includes ex ante measures within the development phase of AI systems, such as conducting data protection impact assessments (DPIA) and implementing appropriate technical and organizational measures to help implement the data protection principles, also called data protection by design.

This means that developers of AI systems have a duty to build in safeguards that provide for a guarantee to uphold the data protection principles in the first place. In light thereof, three issues arise.

Fundamental Rights and GDPR

First, the concept of personal data in Art. 4, para. 1, of the GDPR is very broad and has been further expanded by the Court in cases like YS and Others, Nowak, and Breyer (Court of Justice: judgment of 29 June 2010, case C-28/08, Commission v. Bavarian Lager, paras 49-50; judgment of 20 December 2017, case C-434/16, Nowak, paras 54-55; joined cases C-141/12 and C-372/12, YS and Others, paras 45-47).

Hence, it is not exhaustively defined what personal data is which may make it difficult to determine the bounds of AI use for data processing purposes. This is problematic because AI systems cannot necessarily be simply aborted if they become independent, hence, the bounds of AI use should be determined in the development phase already. On the other hand, a broad concept of personal data guarantees to cover nearly all eventualities and thus reflects a technological reality. The very fact that a piece of information has been created or merely distributed by an individual may provide some clues about who that individual may be and AI is able to detect such correlations better than humans.

Fundamental Rights and GDPR (AI discrimination)

Lastly, regarding AI discrimination, the GDPR's prohibition of the processing of special categories of personal data – meaning data that also constitute potential grounds for discrimination – by solely automated means offers a concrete protection against AI discrimination. Unfortunately, the special categories of personal data laid down in Art. 9, para. 1, of the GPDR do not include the categories of colour, language, membership of a national minority, property, and birth which are, however, recognised as grounds of discrimination in Art. 21, para. 1, of the Charter. This constitutes a potential gap in the prevention of discriminatory results through personal data processing, both by AI systems and conventional means.

Fundamental Rights and GDPR (AI discrimination)

Moreover, Art. 22, para. 1, GDPR, further underlined by Art. 35, para. 3, prohibits profiling by fully automated means. Profiling is a form of processing carried out on personal data to evaluate personal aspects about a natural person and, as the name says, create profiles. This process places people in categories based on their personal traits and is thus likely to lead to discrimination. More specifically, data subjects are likely to be objectified because AI systems evaluate individuals by the probability of a group based on correlation and statistical models and thus do not regard individuals in light of their own rights. The prohibition in Art. 22, para. 1, GDPR provides for guarantees against such discrimination. However, the data subject's specific consent constitutes an exception to the prohibition whereby the same issues surrounding specific consent as explained above may arise, thus rendering the protection granted by Art. 22, para. 1, of the data subject's rights inefficient.