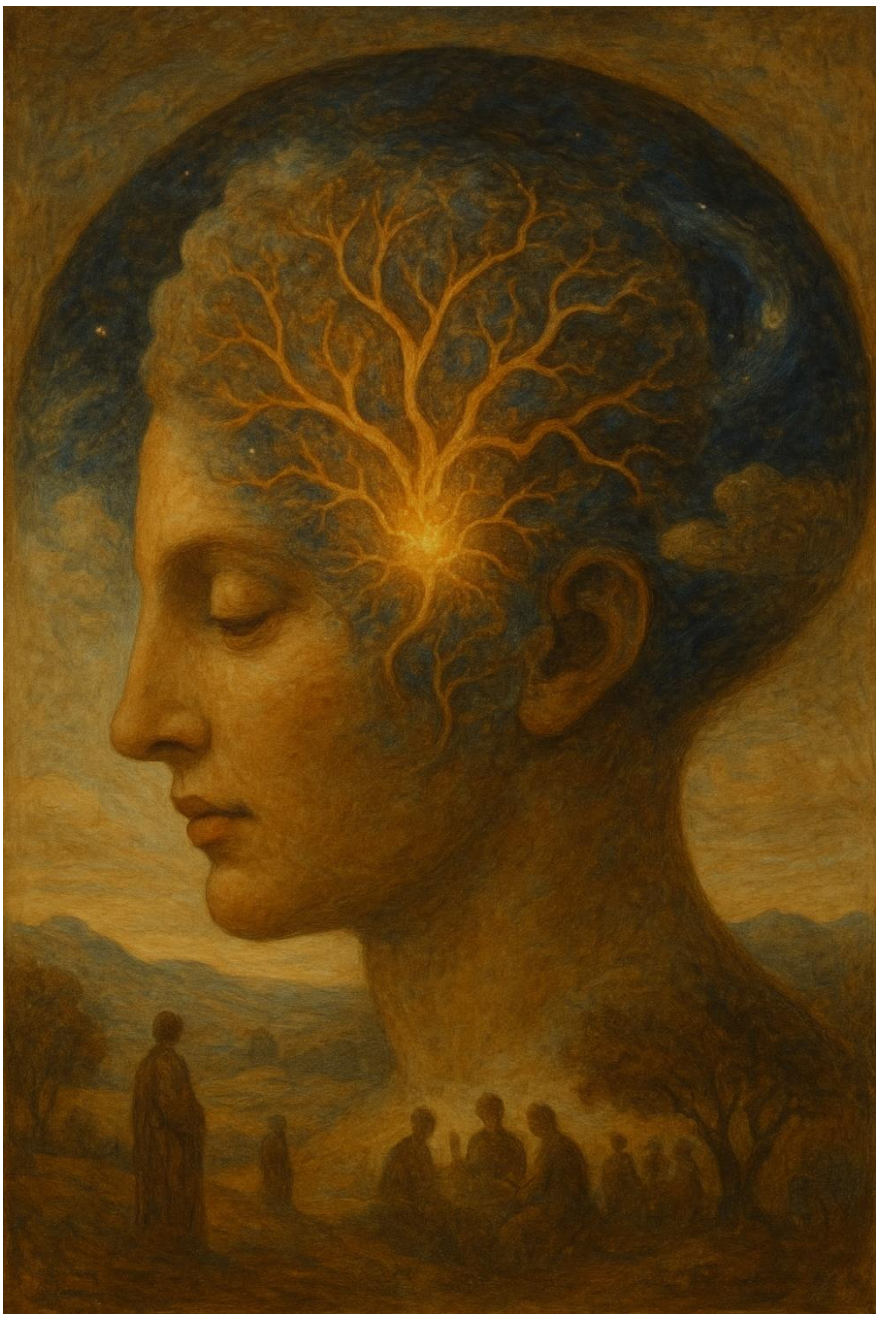
AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

Artificial Intelligence



PART II

Committee on Artificial Intelligence Report, 2026

Table of Contents

Executive Summary

This Report constitutes the first comprehensive contribution of the Committee of Experts on artificial intelligence established by the Italian Communications Regulatory Authority (AGCOM). The Committee was tasked with analysing the legal and regulatory issues that the Authority will have to address in the short and medium term, in a context marked by profound technological transformation and by a European regulatory framework that is still evolving substantially.

The Report is structured into seven chapters, each entrusted to one or more experts from the Committee, and concludes with a synthesis chapter on the prospects for the regulation and governance of generative AI. The main contents and recommendations emerging from the individual contributions are summarised below.

The introduction, by **Andrea Renda**, examines the "crisis phase" of the European AI Act. Conceived as a pioneering instrument for the regulation of artificial intelligence through a risk-based approach, the Regulation underwent a radical transformation following the emergence of general-purpose AI systems (GPAI). The market launch of ChatGPT in November 2022 forced the European co-legislators to reopen negotiations, introducing a specific set of rules for GPAI and a new governance system centred on the European Commission's AI Office. The final text nevertheless suffers from structural gaps in adaptive governance and is subject to growing pressure towards deregulation — both internally (the proposed *Digital Omnibus*) and internationally (the stance of the US administration). The chapter identifies three fundamental areas of weakness: the absence of a sufficiently flexible regulatory architecture, the hybrid and not fully applicable nature of the legislation, and the lack of an adequate interface between the European regulator and national sectoral authorities — including AGCOM. The contribution by **Giovanna de Minico** (Chapter 2) reconstructs AGCOM's competences at the intersection between the Digital Services Act (DSA) and the AI Act. Although the Authority has not been expressly designated as an AI supervisory authority, it may exercise its enforcement powers — supervision, orders and sanctions

— whenever AI systems, and in particular LLMs, are used as vectors for illegal content on digital platforms falling within its remit. AGCOM's competence is derived from its status as Digital Services Coordinator (DSC) under the DSA, which grants it powers of intervention in relation to phenomena such as disinformation, hate speech, covert advertising and infringements of information pluralism. The contribution also examines AGCOM's competences in the field of online political advertising (Regulation (EU) 2024/900), highlighting the shortcomings of a regime limited to transparency obligations, which neither introduces quantitative limits nor prohibits emotional manipulation techniques. A broad theoretical analysis of the relationship between technology and law — understood as the "mosaic of rules in the digital ecosystem" — completes the contribution, examining the conditions for the constitutional legitimacy of self-regulation and the risk that technology may replace politics as a source of law.

Chapter 3, by **Andrea Imperiali di Francavilla,** offers a systematic and operationally relevant mapping of the impacts of AI across all sectors falling within AGCOM's remit: electronic communications, digital services and audiovisual media, postal services and consumer protection. For each sector, actual and potential impacts, intervention priorities and available regulatory tools are identified (ex ante, in itinere, ex post). In electronic communications, the urgent risks include algorithmic discrimination in data traffic (*throttling*, dynamic *zero rating*), algorithmic price collusion and the loss of human control in network management. In the media sector, the chapter highlights threats to pluralism posed by recommendation algorithms, the proliferation of deepfakes and the need for a mandatory labelling regime for AI-generated content. The chapter includes a comparative benchmark of the main European regulators (Ofcom, Arcom, BNetzA, BEREC, ERGA) and a reconstruction of the applicable regulatory mosaic (AI Act, DSA, GDPR, Digital Omnibus), with operational guidance for AGCOM on how to build internal technical capacity, independent testing tools and permanent monitoring systems.

In Chapters 4 and 5, **Andrea Simoncini** and **Giovanni Boccia Artieri** analyse the constitutional dimension of the challenge posed by AI to democracy and freedom of information. Digital platforms, configured as "social formations" exercising private

normative power on a global scale, redesign the information and public-discourse ecosystem in a manner that is difficult to reconcile with the principles of liberal constitutionalism. Simoncini's chapter examines the case of Romania as a "constitutional laboratory" for the implications of AI for democratic sovereignty, and advocates an approach of "European digital constitutionalism" capable of binding platforms to respect fundamental rights and rebalancing the relationship between private power and the public sphere. Boccia Artieri examines the systemic risks associated with the use of generative AI as a "cognitive infrastructure" of public discourse. AI is no longer merely a technical tool but an epistemic environment that redefines the criteria of credibility, truth and authority. The chapter identifies three main vectors of risk: information manipulation (deepfakes, voice cloning, scalable synthetic disinformation), discursive degradation (algorithmically amplified hate speech) and the mechanisms of the attention economy. For each risk, specific regulatory tools are proposed — from *provenance* and *labelling* systems to rapid-response protocols for harmful content — recommending that AGCOM position itself as an "infrastructure of trust" in the Italian communications landscape.

In Chapter 6, **Giuseppe Cassano** reconstructs the issue of authorship and copyright protection in an ecosystem dominated by generative AI. The chapter examines the evolution of the Italian, European and comparative regulatory framework in relation to works created with the assistance of AI — essentially distinguishing between human intellectual contribution and autonomous generation by the machine. Italian Law No. 132/2025 on artificial intelligence extends copyright protection to works that reflect the author's intellectual work, even if assisted by AI. The chapter also analyses the implications of training models on copyright-protected datasets and identifies the Code of Good Practice for AI as an instrument for balancing creators' rights with the development needs of AI systems.

In Chapter 7, **Mauro Giusto** addresses the educational dimension of the challenge posed by AI, starting from the "paradox of the most connected yet least aware generation". Young people are exposed to specific risks — from educational dropout to harm to identity, from technological dependence to exposure to deepfakes — which

require a systemic response involving schools, families, businesses and institutions. The chapter proposes the concept of "algorethics" — education in critical reasoning in the age of algorithms — as a compass for public policies on digital literacy, and identifies AGCOM as a key actor in promoting standards for the protection of minors in the digital ecosystem.

Lastly, Chapter 8 (by **Giovanna de Minico**) explores, from a constitutional law perspective, the relationship between technology and law in the age of AI, offering an original reflection on the risk that technology may replace politics as an autonomous source of law. Starting from a philosophical genealogy that runs from Aeschylus to Aristotle and through to contemporary digital markets, the chapter shows how technology has progressively eroded the primacy of legal norms: from an instrument serving politics, it has become an autonomous — and often opaque — normative actor, intervening with increasing force and limited democratic legitimacy on the very objects of law. The chapter analyses three mechanisms through which technology penetrates the system of sources: (i) the discretionary completion of "open" antitrust rules through technical parameters defined case by case by the Authority, assigning to the Antitrust authority a hybrid function between *iuris dictio* and political direction; (ii) the transformation of private self-regulation into a source of law in the digital ecosystem, together with the conditions of constitutional legitimacy that such source-codes must satisfy in order not to degenerate into forms of uncontrolled private power; (iii) the risk that AI systems may directly become a *source of law*, issuing concrete and particular determinations that erase legal certainty, perpetuate algorithmic injustices and replace the *rule of law* with the *rule of tech*. The analysis of the DSA shows how the voluntary codes provided for therein risk failing to meet the conditions for constitutional compatibility, while the AI Act — despite its ambition to orient technology towards human beings — relies excessively on providers' self-declarations, foregoing impartial public controls. The concluding proposal rehabilitates the Aristotelian principle of the primacy of politics over technology, recast in a supranational European key: the EU legislator must do less (eliminating outdated and intrusive rules) but differently (rewriting AI regulation by prioritising impartial public controls and introducing adequate structural remedies against the dominance of major

digital operators). Only under these conditions can the intertwining of technology and politics become a factor in the growth of the democratic legal order, rather than a vector of its erosion.

On the basis of the contributions collected, the Committee formulates the following priority recommendations for AGCOM:

- **Strengthen internal technical capacity:** Invest in a dedicated team of AI auditors, data scientists and specialised lawyers, capable of conducting autonomous algorithmic inspections and developing independent testing tools modelled on the experiences of Ofcom and BNetzA.
- **Enhance institutional coordination:** Enter into formal cooperation protocols with AgID, ACN, the Data Protection Authority and AGCM, ensuring coherent and proportionate enforcement of the European regulatory framework on AI in the respective areas of competence.
- **Establish a permanent AI Observatory:** Create a system for the continuous monitoring of the impacts of AI in regulated sectors, with public *dashboards*, periodic reports and automated tools for detecting *bias*, discrimination and violations of information pluralism.
- **Adjust the sanctions system:** Activate the sanctions provided for by the DSA (up to 6% of global turnover) and by the AI Act (up to 7%), overcoming the structural limits of Law No. 249/1997, which make enforcement insufficiently deterrent in relation to operators' turnover.
- **Develop a modular regulatory framework:** Develop sectoral codes of conduct, guidelines and algorithmic-transparency obligations harmonised across the different areas of competence, based on common principles adaptable to technological evolution (transparency, *human oversight*, non-discrimination, protection of vulnerable persons).

- **Actively participate in European networks:** Contribute proactively to BEREC and ERGA working groups, co-developing common tools for AI auditing and for the harmonisation of enforcement practices at European level.
- **Experimentation and SupTech:** Launch experimentation with *supervisory technology* (SupTech) tools for the automated monitoring of regulated markets, paving the way for forms of enforcement based on real-time data rather than periodic inspections. AGCOM should also establish a *regulatory sandbox* dedicated to AI systems operating in the sectors within its remit — electronic communications, audiovisual media, digital and postal services.

1 Introduction. Artificial Intelligence as an opportunity and responsibility for independent authorities

Andrea Renda

A thorny and constantly evolving subject, Artificial Intelligence (AI) continues to disturb the sleep of many legislators and regulators around the world. Moreover, while some countries appear increasingly reluctant to adopt legislative instruments to address the rapid advance of AI — which permeates industrial sectors, research and science, as well as public life and government — the risks associated with the uncontrolled spread of the most powerful AI models are becoming more evident by the day. An attentive observer cannot fail to notice the current dispute between the US government (in particular the Department of Defense — or, in Trump-era terms, the Department of War) and companies such as Anthropic, which are concerned about the indiscriminate use that the military, or the Department of Homeland Security increasingly devoted to mass surveillance, may make of their extremely powerful models. A *querelle* which, in the absence of clear and effective regulation, can only give rise to races to the bottom, as shown specifically by the opportunism of Anthropic's main rival, OpenAI, ready to accept the Trump administration's unconditional requests in disregard of the most basic ethical principles and *guardrails*. Nor can the more attentive eye overlook the dynamics of data, water and energy consumption by so-called frontier models, on which the most advanced companies spend hundreds of billions of dollars a year while waiting for demand and applications that do not yet seem to be on the horizon. Lastly, with regard to *killer apps*, an attentive (and critical) observer cannot overlook the use being made of so-called Large Language Models in the military field, as powerful tools of disinformation (consider the latest trend, *LLM grooming*) and as formidable allies of *hackers* in cyberattacks.

In Europe, these and other trends have generated widespread demand for a reconsideration, *à rebours*, of a legislative path that had so far stood out for its ambition and clear orientation towards the protection of fundamental rights, as well as the safety of products and services using Artificial Intelligence. This reconsideration has deep roots and includes the significant pressures that EU institutions have faced in recent months from the US government, as was already evident in the speech delivered by Vice President J.D. Vance at the Paris AI Action Summit in February 2025. The speech was entirely oriented towards deregulation, with the aim of removing any obstacle to the development and deployment of AI, and was accompanied — perhaps unwittingly — by the European Commission's decision not to pursue the proposed directive on civil liability in the age of AI, pending since September 2022.[1] This reconsideration also fits with the renewed imperative that dominates the agenda of the new European Commission: competitiveness and regulatory simplification, evoked by the Draghi Report as early as 2024 and resulting in a series of so-called *omnibus* legislative proposals, including one on digital matters that aims, among other things, to simplify the AI Act and the regulation on personal data protection.

This reconsideration, to be clear, is partly warranted, although not for the reasons set out so far. To understand why, however, it is necessary to take a step back to the gestation phase of the AI Act. Born of the 2020 White Paper on artificial intelligence, which explicitly aspired to create an ecosystem "of trust" and one "of excellence" in this field, the AI Act — at least in the original version proposed by the European Commission — translated into legal terms the guidelines on trustworthy AI prepared by the High-Level Expert Group appointed by the European Commission some years earlier, in 2018. By adopting a risk-based approach, the AI Act introduced a four-level taxonomy which — while remaining firmly anchored in the principle of not regulating technology as such — aimed to exclude excessively risky applications from the market and focused on regulating a limited number of applications deemed "high risk" in terms of violations of fundamental rights or safety. In an approach that, although denounced as excessively interventionist, was in fact minimalist, the proposed regulation relied on

[1]European Commission – proposal for Directive COM(2022) 496: AI Liability Directive on the non-contractual civil liability regime applicable to artificial intelligence.

product-safety law as its legal basis and subjected high-risk AI applications to the European (co-)regulatory framework requiring the affixing of the "CE marking" as a prerequisite for circulation in the internal market. Moreover, in most cases under the *AI Act* the verification of the conformity of high-risk applications with regulatory requirements remains subject to "internal controls" by providers, and only in a minority of cases was the involvement of third parties envisaged, as provided for under European CE-marking legislation.

1.1 The "crisis phase" of the AI Act

Although pioneering and controversial from the outset, the initial version of April 2021 in fact represented a rather timid intervention: minimalist in scope, cautious in imposing *compliance* costs, and accompanied by rather thin governance. The proposal was notable for a technology-neutral definition of AI, capable of constant updating given the unceasing evolution of the subject matter; regulatory requirements defined in fairly vague terms, to be interpreted case by case; a possibility — albeit limited, and in the view of many limiting — to revise the taxonomy of risk applications placed in an annex to the proposed regulation so as to allow more agile review; and the introduction of *regulatory sandboxes* governed at national level to facilitate market access and the verification of regulatory compatibility, especially for small and medium-sized enterprises. The proposed AI Act, presented during the pandemic, generated great international interest, with countries such as South Korea, Brazil, Canada and Colombia initially determined to emulate its approach and essential content. It was not, however, an entirely horizontal approach, in the sense of being generally applicable to all AI sectors and *use cases*. On the contrary: on the one hand, the risk-based approach focused on a number of applications that the Commission estimated to account for less than 10% of the market; on the other, some AI-specific problems, such as disinformation and content moderation on social networks, fell outside the scope of the Act, given the almost contemporaneous introduction of the Digital Services Act. The latter can, for all intents and purposes, be counted among the EU's legislative measures on artificial intelligence: nevertheless, the systemic-risk analysis by third parties envisaged therein for AI systems used by very large platforms and search engines still awaits adequate reconciliation with the conformity-assessment procedure provided

for by the AI Act, not to mention the risk analysis envisaged for general-purpose AI systems, which will be discussed shortly.

Those years, 2021–2022, were fertile days for the debate on AI regulation. Apart from the rather evident traces of an incipient *Brussels effect*, which filled Brussels officials with pride, there was a gradual revival of international cooperation, starting with standardisation bodies (ISO, IEC, IEEE) and extending to contexts such as the OECD, the Global Partnership on AI (GPAI), the G7 and the G20, and gradually also the United Nations thanks to the so-called Global Digital Compact and the Pact for the Future.

However, in this springtime of regulation, two crucial factors ultimately "broke the toy" of the AI Act. The first coincides with the gradual realisation of the complexity and constant transformation of the subject matter being regulated. As early as September 2022, Engler and Renda (2022) had highlighted that the AI Act's emphasis on the so-called "provider" — the entity that places the AI system or model on the market, or puts it into service under its own name or trademark — was ill-suited to a market structure that was becoming concentrated in the hands of companies developing versatile systems and offering them to *downstream* providers with limited knowledge of the design and development specifications of the models themselves. In other, more straightforward words, focusing on the provider meant missing the target and placing on the shoulders of the least informed party — certainly not the so-called *cheapest cost avoider* — the responsibility for ensuring that the AI application complied with the regulatory requirements of the AI Act. While the European Parliament hurried to introduce cooperation obligations along the AI value chain, between *upstream* actors and providers, the market launch of ChatGPT in November 2022 definitively confirmed the need to intervene in a much more structural way in the conceptual and legal architecture of the AI Act. Shortly afterwards, in February 2023, the co-legislators decided to reopen negotiations on the text of the Regulation, triggering a trilogue that would substantially modify its architecture.

What emerged was a text very different from the original proposal, with a *corpus* of rules tailored to so-called *General Purpose AI Systems (GPAI)*, or general-purpose AI systems, for which asymmetric regulation was envisaged, similar to that established by the Digital Services Act, with stricter obligations for providers of particularly powerful

GPAI, and therefore capable of generating systemic risks. These rules were accompanied by a completely new governance system, additional to that envisaged for high-risk applications and subject to the competence of the European Commission, within which a new service, the AI Office, was created. This was by no means an obvious *upgrade*, but rather the result of growing awareness of the incompleteness of the original framework. Moreover, the final text saw the light of day in the silence of the trilogue, and therefore in the total absence of public consultation or input from experts. The sense of urgency that accompanied the radical reform of a text that had not yet entered into force vividly illustrates the *impasse* of the European regulator, grappling with a fluid subject matter whose phenomenology is almost unpredictable.

The need to accelerate the EU regulator's initiative also materialised in renewed activism on the *soft law* front, with the Commission seeking a broad agreement that could anticipate the entry into force of the essential rules of the AI Act. This led to the AI "Pact", signed by dozens of companies as a preliminary commitment to the responsible development of AI; and to the laborious Code of Conduct on GPAI, produced after a long and difficult gestation by a group of experts which, after exceeding a thousand participants, ultimately relied on the (competent) pens of about a dozen experts. Subsequently, a profusion of guidelines and delegated acts issued by the Commission on various aspects of the AI Act helped to clarify, at least in part, the obligations of actors such as providers of GPAI and of *high-risk* applications, how to define and identify such applications, and many other general aspects that are not easy to interpret in the text of the Regulation.

These efforts became even more heroic during 2024 and 2025, because of a second set of factors that had a far from negligible impact on the complexity of the European regulatory project. On the one hand, the progressive realisation of Europe's limited competitiveness in the field of AI, in the face of dizzying advances in the United States and China, convinced the European Commission — especially at the beginning of Ursula von der Leyen's second term — to pursue a path of regulatory simplification, at times turning into attempts at deregulation, in response to the heartfelt appeal of the "Draghi Report". Of the two ecosystems originally contemplated by the 2020 White Paper, the excellence ecosystem appeared deficient, while the trust ecosystem still

seemed far from full completion. Hence the decision to abandon the civil-liability directive project already mentioned, and to introduce a simplification proposal — the so-called *Digital Omnibus* — which further modifies the scope and application of the AI Act, once again without relying on a genuine regulatory impact assessment.

On the other hand, this renewed — entirely home-grown — vocation for deregulation was accompanied by international pressure exerted by the US administration, determined not to support any attempt at international cooperation on *regulation* in this field and ready to make the "simplification" of European regulation a bargaining element in the face of an unusually aggressive trade-tariff policy. Legislation such as the AI Act and the DSA thus found itself in the dock, in an alignment of intentions that significantly weakened both the impetus to complete the *opus magnum* of the AI Act and processes of international cooperation on AI, with the sole exception of the rather ineffective Hiroshima process, still active — albeit with little force — within the G7.

Lastly, it is useful to recall that the process of applying the AI Act depends significantly on the completion of a parallel path: standardisation, the subject of a specific mandate that the Commission addressed to CEN-CENELEC. So far, this process has proved rather cumbersome and marked by conflicts of interest, considering that private companies are called upon to define standards which, once validated, will apply to those very companies; and that roughly half of the Member States have expressed, within the EU Council, support for a significant downward redefinition of the scope of the AI Act. Faced with the problem, in the *Digital Omnibus* the European Commission ultimately officially postponed the application of the rules on high-risk applications by one year, until August 2027. Even then, it found itself having to announce that, in the absence of sufficiently detailed standards produced by CEN-CENELEC, it would be forced to introduce provisional standards, the development of which would involve no small difficulties.

1.2 A work destined to remain unfinished?

In the face of so many difficulties, the trajectory of the AI Act appears today to have lost its initial momentum, for various reasons which I shall try to summarise here, without claiming to be exhaustive.

First, despite the Commission's initial effort, the text lacks some fundamental elements that would make the AI Act more flexible and able to withstand the advance and continuous evolution of AI. While, on the one hand, the definition of AI is technology-neutral, the lists of applications initially placed in the four risk categories are conveniently included in annexes to the text, and the *regulatory sandboxes* (see Chapter 6 of this Report) promise openness to innovation especially for SMEs, on the other hand the regulatory architecture lacked genuine adaptive *governance*, in the form of a European agency supported by a group of experts capable of guiding its action. From this point of view, it would have been preferable to avoid adopting a text exceeding 250 pages, favouring a more agile intervention focused on the principles and objectives of the regulatory measure, and more centred on entrusting an independent *governance* body with the constant updating of the state of the art in AI. This would have allowed a more streamlined approval and entry-into-force process, as well as a faster, more flexible and more participatory regulatory framework. It would also have enabled the independent European authority to begin cooperating immediately with sectoral regulators, which — as we shall see — play an essential role in making the Regulation effective.

Second, in oscillating between principles-based regulation and prescriptive legislation, the AI Act ultimately lands halfway: too detailed to be agile, and too little prescriptive to be immediately applicable. The cause of this indeterminacy lies in the very nature of the problem — at once transient and pervasive — which forces the European regulator to constantly undertake regulatory revisions in order to correct them even before they take effect. One need only read the text to realise this: the regulatory requirements associated with high-risk applications are necessarily generic and difficult for regulated entities to apply. The reason is simple: not only does the list of high-risk applications include use cases clearly linked to safety issues and risks to fundamental rights; in addition, each sector and *use case* presents risks of different kinds and magnitude, as well as very different risk-mitigation measures. Referring, for example, to adequate human oversight is not enough to explain what the requirement entails for a hospital *triage* system, the use of an AI system in a judicial context, or an autonomous

vehicle. The same applies to each of the requirements, which must be translated into more concrete guidance for each future application.

Hence, as a third factor, the need emerges to establish an adequate "interface" between the European regulator and the authorities competent for specific matters, such as data-protection authorities; and even more so sectoral regulatory authorities, whether governmental bodies or independent authorities. These institutions, often forgotten in the European and international debate, are called upon to reconcile the legislation for which they are competent with the provisions of the AI Act, and more generally with the spread of AI in the products and services whose supervision falls within their remit. The great forgotten actors of the first season of the AI Act, data-protection and sectoral authorities may now return to the forefront as protagonists of a second season, in which the breathless race to keep up with the constant evolution of AI is replaced by a more considered approach to the regulatory reforms needed to ensure that specific legislation remains *fit for purpose* in the age of the most advanced AI. In this context, they will encounter interlocutors that are different and not necessarily aligned, considering that for certain types of applications they will have to refer to the national context; but also that, especially if the Digital Omnibus proposal were to become law, they will be joined by the European Commission and the AI Office, which, through the omnibus, announce their intention to provide greater legal certainty regarding the overlap between the AI Act and other European rules, and propose centralising within the AI Office the supervision of AI systems developed from GPAI or used by large platforms or search engines (as defined by the DSA).

This is, as noted, a proposal subject to scrutiny by Parliament and Council. If it were to "pass", it would mean another sudden change for the AI Act enforcement system, as well as a shift in scenario for national supervisory authorities. It would almost amount to a "normalisation" of the AI Act, considering that almost all countries that have decided to develop a public policy on AI have done so by adopting a very thin horizontal regulatory framework, combined with a stronger effort at sectoral regulation.

1.3 Independent authorities in the age of artificial intelligence: rationale and structure of the work

Faced with such an uncertain and changing scenario, supervisory authorities must ask themselves a number of fundamental questions. Which AI Act will they find themselves having to implement? Who will be the main actors, at European and national level, and with what competences? How can they ensure that sectoral legislation fully and dynamically reflects the evolution of AI? To what extent should they rely on national authorities with general competence, where they exist (in many countries, there is no central authority responsible for AI)? And again: which regulatory instruments should be used, and which socio-technical standards should be adopted as reference points?

It is in this context that AGCOM decided to create an independent Committee of AI experts, with strong legal expertise, tasked with identifying and analysing the legal issues that AGCOM will have to address over the coming months and years, as well as identifying the opportunities that AI can offer both in the market contexts falling within AGCOM's remit and as support for the regulatory process itself.

This Report constitutes the Committee's first contribution and consists of nine chapters. In the first contribution, Giovanna de Minico analyses the interrelationship between the AI Act and the DSA, highlights the possible impact of the two pieces of legislation on AGCOM's powers and — in the second part — explores the impact of the European regulation on political advertising. In Chapter 3, Andrea Imperiali di Francavilla presents nothing short of a monumental mapping of the impact of artificial intelligence across all sectors regulated by AGCOM. In Chapter 4, Andrea Simoncini examines the constitutional implications of artificial intelligence for democracy and freedom of information, proposing a model of European digital constitutionalism aimed at safeguarding fundamental rights and rebalancing the relationship between private power and the public sphere. In Chapter 5, Giovanni Boccia Artieri takes stock of a highly topical and thorny issue: generative AI and its impact on disinformation and *hate speech*. Chapter 6, by Giuseppe Cassano, explores the issue — which has become crucial especially in the age of generative AI — of copyright protection. In Chapter 7, Mauro Giusto offers a more systemic view, presenting his reflections on AI and the education of young people. Chapter 8, again authored by Giovanna de Minico, offers a

broader constitutional reflection on the relationship between technology and law, analysing the conditions under which technology risks evolving from a tool governed by law into an autonomous source of normative power and proposing safeguards capable of preserving the primacy of democratic decision-making.

In the concluding chapter, I draw together the previous contributions, combining them with a reflection on current developments in the EU agenda, on the next evolution of AI (starting from *agentic AI* and the uncertainty it is also generating for the application of the AI Act), and on the regulatory and governance instruments that independent authorities will need to adopt in the coming years in order to equip themselves properly for what appears to be an arduous path in the face of an increasingly thorny regulated subject matter.

2 AGCOM regulation around the digital ecosystem

Giovanna de Minico

Summary: Part A): The encounter between the DSA and the AI Act: AGCOM's competences. – 1. The questions raised by the DSA and the AI Act. – 2. What relationship exists between AGCOM's powers under the DSA and the structure of the AI Act? – 3. A possible interpretative key in response to the second question. – 4. Future case studies.
Part B): The European Regulation on political advertising and the reservation of competences to AGCOM. – 1. Lights and shadows of the European Regulation on political advertising. – 2. AGCOM in dialogue with the other Authorities. – 3. Summary table.

2.1 The encounter between the DSA and the AI Act: AGCOM's competences

2.1.1 The questions raised by the DSA and the AI Act

I draw the reader's attention to certain issues that a careful examination of the European and domestic regulatory framework has raised, while at the same time leaving them open, thus entrusting their future definition to the interpreter yet to come.

1) According to the legal framework recalled above, does AGCOM hold specific competences in the field of artificial intelligence (AI)?
2) If the answer to this question were affirmative, what would be the nature of that competence and what matters would fall within its scope of intervention?

In order to answer these questions, it is necessary to start from a combined reading of the Digital Services Act (DSA)[2] and the Artificial Intelligence Act (AI Act)[3], together with the national law of September 2025 on artificial intelligence[4]. These three sources must therefore be interpreted in relation to one another, without yielding to the temptation of simpler, atomistic readings, which are in any event excluded by the systemic nature of the two legal orders, domestic and European, which, by integrating with each other, require each to be considered in the light of the other and vice versa (Betti).

2.1.2 What relationship exists between AGCOM's powers under the DSA and the structure of the AI Act?

Let us turn to the first question.

We know that AGCOM has been designated as the national Digital Services Coordinator (DSC) (Article 49 DSA): it is therefore responsible for the coordination, supervision and application of the DSA throughout the national territory, with regard to hosting providers, online platforms and online search engines below the EU threshold.[5]

Under the DSA, AGCOM has, among other things, the power to request information, prohibit unlawful conduct (through orders) and impose sanctions (for example in the event of non-compliance with orders) on digital service providers operating on the

* Full Professor of Constitutional and Public Law – Department of Law – University of Naples Federico II. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act).

[2] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).

[3]Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No. 300/2008, (EU) No. 167/2013, (EU) No. 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Regulation).

[4] Law No. 132 of 23 September 2025, Provisions and delegations to the Government on artificial intelligence, in Official Gazette No. 223 of 25 September 2025.

[5]To this end, the law establishing the Authority was specifically amended by inserting, in Article 1(6)(c) of Law No. 249/1997, point 14-ter), under which the Authority "performs the function of Digital Services Coordinator and exercises the related powers provided for by Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a single market for digital services". (Article 15(3), Decree-Law No. 123/2023, the so-called "Caivano Decree").

national territory, where the Authority identifies a 'propagation' of harmful content to the undefined mass of users.[6]

AGCOM is therefore the NRA competent ex lege to adopt actions aimed at preventing the propagation of 'illegal content'. It should be noted that the DSA neither provides a definition nor sets out a numerus clausus as regards 'illegal content'. Article 3(1)(h) defines 'illegal content' as 'any information that, in itself or in relation to an activity, including the sale of products or the provision of services, is not in compliance with Union law or the law of any Member State which is in compliance with Union law, irrespective of the precise subject matter or nature of that law'. The Regulation therefore refers dynamically to an external legal parameter (Union or domestic), leaving it to the regulator's discretion to identify, case by case, the rule alleged to have been infringed and which confers the attribute of illegality on the content, in the sense of its conflict with the legal command.[7]

Furthermore, AGCOM (with regard to national platforms) and the Commission (for VLOPs/VLOSEs) are the actors identified by Union and domestic law to counter the dissemination of illegal content, since the mere circulation of such content and the consequent exposure of the user are considered a danger ex se — a feared event —

[6]Articles 9 and 10 DSA concern, respectively, the order to remove illegal content and the order to provide information. In addition, under Article 52, where necessary for the performance of their tasks under the Regulation, Digital Services Coordinators have enforcement powers, i.e. coercive powers in a broad sense (i.e. powers to affect/modify the legal sphere of the person concerned, to be exercised in compliance with the indispensable guarantees of the adversarial procedure) vis-à-vis providers of intermediary services falling within the competence of their Member State. For the detailed list, reference is made to the positive law.

[7]See Recital 12: "In order to achieve the objective of ensuring a safe, predictable and trusted online environment, for the purposes of this Regulation the concept of 'illegal content' should broadly reflect the existing rules in the offline environment. In particular, the concept of 'illegal content' should be defined broadly to cover information relating to illegal content, products, services and activities. That concept should in particular be understood as referring to information, irrespective of its form, that under the applicable law is itself illegal, such as illegal hate speech or terrorist content and unlawful discriminatory content, or that the applicable rules render illegal because it relates to illegal activities. Examples include the sharing of images depicting child sexual abuse, the unlawful non-consensual sharing of private images, cyberstalking, the sale of non-compliant or counterfeit products, the sale of products or provision of services in violation of consumer protection law, the unauthorised use of copyright-protected material, the illegal offering of accommodation services or the illegal sale of live animals. Conversely, a video by an eyewitness of a potential crime should not be considered illegal content merely because it shows an unlawful act, where the recording or dissemination of that video to the public is not illegal under national or Union law. In this regard, it is irrelevant whether the illegality of the information or activity is established by Union law or by national law compliant with Union law, and what the exact nature or subject matter of the law in question is."

even where its dissemination has not produced a concrete and actual harmful effect on the user (an offence of danger).[8]

Hence the assignment to AGCOM of order and sanctioning functions, as well as limited regulatory powers — mainly of an organisational nature — and, finally, coordination functions with the other NRAs (national and European) and with the European Commission itself.[9]

As regards, instead, the European Regulation on AI, together with the national implementing law, a literal interpretation leads to excluding the assignment of express powers to the Authority in question in the field of AI.

Indeed, the AI Regulation provides for a precautionary approach aimed at addressing the so-called systemic risks arising from the use of AI. The national law identifies two specific Authorities, the Agency for Digital Italy (AgID) and the National Cybersecurity Agency (ACN), without conferring specific competences on AGCOM.[10]

It is precisely the national law, however, that provides a useful element for our reasoning. A subject-matter competence could be inferred, by deductive interpretation, where the national law amends copyright law and specifies that content produced by means of AI is also protected by copyright (Article 25(1): 'Law No. 633 of 22 April 1941 is amended as follows: a) in Article 1, first paragraph, after the words "works of the intellect" the word "human" is inserted and after the words "form of expression" the following words are added: "including where created with the aid of artificial intelligence tools, provided they constitute the result of the author's intellectual work"').

It follows that AGCOM, which is competent to protect copyright online directly, could also claim an indirect competence in the protection of products created with the aid of AI.

---

[8]Allow me to refer to one of my works, Nuova tecnica per nuove diseguaglianze. Case law: Disciplina Telecomunicazioni, Digital Services Act e Neurodiritti, in Federalismi.it, 6/2024, p. 17.

[9]As has in fact occurred: see the Regulation on certification of ADR bodies (Article 21 DSA), Resolution No. 282/24/CONS; the Regulation for the appointment of "trusted flaggers" (Article 22 DSA), namely qualified entities authorised to report illegal content to platforms with priority treatment (Resolution No. 283/24/CONS); the Procedural Regulation for handling complaints (Article 53 DSA), Resolution No. 25/25/CONS.

[10]AgID promotes and enables the development of AI, managing notification, accreditation and monitoring activities; ACN, by contrast, supervises the security of AI systems and has control and sanctioning powers, while also promoting cybersecurity aspects related to artificial intelligence.

2.1.3 A possible interpretative key in response to the second question

AGCOM was not created as an 'AI Authority', but it must immediately be said that its extraneousness to the perimeter of the European regulation must come to terms with the reality of Large Language Models (LLMs). This innovative form of AI, so atypical that it was initially ignored by the EU Regulation, has received a legal regime derogating from that reserved to the traditional AI case, given its special nature compared with the general basic model. LLMs enter the Authority's sphere of action, despite the deafening silence of the Regulation and of Italian law, when their use ends up intersecting with the Authority's typical and express competences, because they involve the dissemination of online content; services provided by the platform; information; advertising; and user protection (minors, pluralism, disinformation).

We may exclude that the Authority has powers over AI as an object ex se, which remains outside its sphere of action; however, this does not exclude the possibility that the Authority may intervene in relation to the effects deriving from its use, where LLMs contribute to the propagation of 'illegal' content which, as such, falls within the open category of Article 3 DSA. Therefore, where an LLM is integrated into a social network, a search engine, an information chatbot or recommendation systems, AGCOM must be regarded as being called upon whenever it identifies cases falling within its competence, namely those designed by the DSA and by national laws, for example the TUSMA. By way of example, one may think of the following areas: disinformation; hate speech; violation of the protection of minors; lack of algorithmic transparency or violation of information pluralism.[11]

2.1.4 Future case studies

We shall set out one further case that may help to understand the systematic interpretation proposed here: in the context of digital services, AI is used to moderate content (automatic removal of posts or videos), personalise advertising, detect suspicious or illegal behaviour (e.g. deepfakes, hate speech), and manage chatbots and virtual assistants. This means that, where a provider uses an LLM to generate or

[11] Allow us to refer to: Too Many Rules or Zero Rules for the CHATGPT, in G. De Minico, Libertà Virtuali. Costituzione e Mercato, Merita Edizioni, Turin, 2024, p. 246.

amplify illegal content, AGCOM may request information, assess risks, impose corrective measures and impose sanctions for lack of transparency or inadequate moderation.[12]

In the field of advertising and commercial communications, AI may be used for forms of automated influencer marketing, and this may open up spaces for action by AGCOM where forms of covert advertising are being carried out.

Therefore, the Authority does not act directly on AI, because no source assigns it this task, nor does it have regulatory powers. Here we must apply the criterion of formal legality strictly, which leads us to exclude its competence because AGCOM, like any other public authority, must comply with the principle of legality: it must be able at all times to exhibit an ad hoc legal title justifying the powers it intends to exercise. Legality for public power is expressed positively as the exhibition of a prior legal rule which, as a rule of action, confers the attribution that the Authority claims as its own, unlike the sector governed by private law, where the rule applies that everything not prohibited by law is lawful for the individual. That said, there is a 'but': a careful analysis reveals that AGCOM may rely on its enforcement powers — supervision and control, orders, sanctions — when AI becomes the means, that is, the technology used by platforms to offer illegal services and content to end users. In this context the Authority will rely solely on its typical functions, which, by affecting the content hosted by the platform, will also indirectly intercept the product created by the LLM, while substantially respecting the principle of formal legality. Here we have not resorted to the theory of implicit powers — whose constitutional compatibility with the principle of formal legality is extremely delicate — because we have not inferred an unexpressed and lesser power from an expressed and greater one; rather, we have merely widened the compass held by the Authority over all material hosted by the platform, whether generated by users who post it or by a mechanical mind that generates it autonomously.

Let us therefore move rapidly to the conclusions, emphasising two further profiles.

[12]Id., Unione europea, mercato, tecnica, paper presented at the annual conference of the Italian Association of Constitutionalists, "The European Union in comparison with the Constitution of the Italian Republic", University of Turin, 11/10/2025.

It is clear that the exercise of these functions could give rise to overlaps of competences, which consequently entails the need for the various NRAs involved to coordinate, in accordance with the European method of sincere cooperation.

For example, if content harmful to minors is transmitted through a channel broadcasting AI-generated content, AGCOM is competent to intervene under the DSA (and also under national sources, for example the TUSMA and the Caivano Decree); if the same content also violates the minor's privacy (for example by showing the face of a minor), the intervention of the Data Protection Authority will also be necessary. If, within the same conduct, potential risks to the overall security of the Network are also identified, ACN's powers will also come into play. The instrument of coordination among NRAs through the conclusion of cooperation protocols therefore represents an indispensable step for the proper functioning of administrative action, as some of us have long suggested.

Finally, this enforcement power and the resulting sanctioning function intersect with the major issue of platform liability. The e-commerce Directive, not amended on this point by the DSA, provides for a conditional liability regime for platforms: if they are unaware of the harmful content transmitted, or if they remove it as soon as they become aware of it, the platform is deemed not liable. However, the DSA preserves the platform's duty of care to prevent harm: the platform must in turn equip itself with an internal organisational system capable of preventing the uncontrolled dissemination of illegal content, including through AI systems (see Council of State, No. 4277/2024). If the platform fails to act in this way, or does not demonstrate that it has adopted such systems, in litigation it cannot be considered to have discharged the burden of contrary proof.

We welcome the recent administrative case law which — in order to counter the network Giants' self-exemption from liability based on the myth of the neutrality of the hosting provider — has elevated AI management systems (aimed at preventing harm) to an essential organisational element for demonstrating fulfilment of the platform's duty of care.

In this context, AI makes a qualitative leap: technology is no longer merely the means of disseminating potentially harmful content, but becomes the privileged instrument for containing the feared harm.

2.2 The European Regulation on political advertising and AGCOM's competences

2.2.1 Lights and shadows of the European Regulation on political advertising

This Regulation was adopted in response to the self-regulation that had so far prevailed at the initiative of search engines, social networks and platforms. The Regulation follows the philosophy of disclosure, although not in full, since it essentially imposes a transparency obligation limited to certain information on the sponsor of political advertising. This obligation requires the affixing of a label clarifying that the message is advertising and identifying the sponsor, namely the person or entity benefiting from it. But nothing is said about who finances the campaign — a point on which there is silence — and, above all, there is no prohibition on adding advertising space beyond a certain limit.[13]

In short, the Commission has contented itself with informing citizens that they are about to be bombarded with political advertising messages in favour of those who can afford them, without however protecting their right to receive pluralistic information, that is, information contributed by the many political families that articulate the ideological pluralism of society.

The question we ask, therefore, is whether a regulation on advertising that lacks the two essential elements highlighted above can be described as politically useful.

To these two serious omissions must be added a fundamental issue: the exploitation of emotional techniques to steer public opinion in a particular direction. This issue too has not been addressed, just as it is not addressed in the AI Act in Articles 5 and 50.[14]

[13]Allow us to refer to what has already been submitted in: Le fonti del diritto: un argine all'intelligenza artificiale?, in Rivista AIC, 3/2025, 78 ff.

[14]See Id., Nuova tecnica per nuove diseguaglianze, cit., pp. 19-21.

2.2.2 AGCOM in dialogue with the other Authorities

For the purposes of this analysis, in order to identify whether there is room for AGCOM to intervene and how broad that room may be, it is useful to note that the national Data Protection Authority and the European Data Protection Supervisor are competent under Articles 18 and 19 to process data for targeting purposes.

Member States, instead, designate the authorities responsible for monitoring compliance with the obligations on political advertising imposed on providers of intermediary services (as defined by the DSA). That authority may coincide with the one designated under the DSA; in Italy, this has occurred by assigning this task to AGCOM.

The Digital Services Coordinator (DSC), referred to in Article 49 of the DSA, is in fact competent for coordination at national level between the two regulations (political advertising and the DSA). Compliance with the rules in Articles 7 to 21 is entrusted to the supervision of the same authorities designated under the DSA (AGCOM), with the clarification that the Digital Services Regulation limits the governance of national authorities to entities other than VLOPs or VLOSEs.

Consequently, by virtue of the reference made by Article 22 to the DSA framework, the competent authority for online advertising is the European Commission where a VLOP is involved; where, instead, smaller entities are involved (such as a 'neighbourhood blog'), competence remains with the national authority. In the event of violations relating to data processing, the reference authority is the national or European Data Protection Authority.

2.3 Summary table

AGCOM's powers pursuant to Regulation (EU) 2024/900	
Regulation (EU) 2024/900	Comment
Article 22 Competent authorities and contact points 1. The supervisory authorities referred to in Article 51 of Regulation (EU) 2016/679 or the European Data Protection Supervisor referred to in Article 52 of Regulation (EU) 2018/1725 are competent to monitor the application of Articles 18 and 19 of this Regulation within their respective fields of competence. Article 58 of Regulation (EU) 2016/679 and Article 58 of Regulation (EU) 2018/1725 apply mutatis mutandis. Chapter VII of Regulation (EU) 2016/679 applies to the activities covered by Articles 18 and 19 of this Regulation. 2. The European Data Protection Board referred to in Article 68 of Regulation (EU) 2016/679 shall draw up guidelines, on its own initiative or at the request of the Commission, in order to assist the supervisory authorities referred to in Regulation (EU) 2016/679 in assessing compliance with the requirements of this Regulation. 3. Member States shall designate the competent authorities responsible for monitoring compliance, by providers of intermediary services within the	1. AGCOM, as Digital Services Coordinator under the DSA, could be designated at national level as the competent authority to monitor compliance by providers of online intermediary services with Articles 7 to 17 and Article 21, that is, transparency obligations and those relating to the duty of diligence for political advertising services, as well as provisions relating to the legal representative; at present, however, this cannot be stated definitively because the national designation act is awaited. 2. The competence of the Data Protection Authority for targeting under Article 22 remains unaffected.

meaning of Regulation (EU) 2022/2065, with the obligations laid down in Articles 7 to 17 and Article 21 of this Regulation, where applicable. The competent authorities designated under Regulation (EU) 2022/2065 may also be the competent authorities designated to monitor compliance by online intermediaries with the obligations laid down in Articles 7 to 17 and Article 21 of this Regulation. The Digital Services Coordinator referred to in Article 49 of Regulation (EU) 2022/2065 of each Member State is responsible for coordination at national level in relation to providers of 'intermediary services' as defined by Regulation (EU) 2022/2065. Articles 49, 58(1) to (4), and 60(1) of Regulation (EU) 2022/2065 apply to matters connected with the application of this Regulation to providers of intermediary services. Article 51 of Regulation (EU) 2022/2065 applies mutatis mutandis as regards the powers of the competent authorities designated pursuant to this paragraph. 4. Each Member State shall designate one or more competent authorities responsible for the application and enforcement of the aspects of this Regulation not covered by paragraphs 1 and 3 of this Article. Those competent authorities may be different from those referred to in paragraphs 1 and 3 and may be the same as those referred to in Article 30 of Directive 2010/13/EU. Each competent authority designated pursuant to this paragraph shall enjoy full structural independence from the sector and from any external intervention or political pressure. Acting in full	3. In residual matters, a third authority may be identified, including one different from the previous authorities. 4. This clarity in the allocation of competences among national authorities is not also found in the DSA, which assigns to the Digital Services Coordinator the power to request information on the algorithm and therefore also on targeting (Article 40 DSA and Recital 110).

independence, it shall effectively monitor and take the necessary and proportionate measures to ensure supervision, compliance and enforcement of this Regulation. […] 8. The national contact points designated by Member States pursuant to paragraph 9, second subparagraph, shall meet periodically at Union level in the network of national contact points. The network of national contact points acts as a platform for the regular exchange of information and best practices, as well as for structured cooperation between national contact points and the Commission on all aspects of this Regulation. In particular, the network facilitates Union-level cooperation on the application and enforcement of this Regulation and facilitates the development, in cooperation with relevant stakeholders, of guidance intended to assist sponsors and political advertising service providers in complying with the requirements of this Regulation. The network meets at least twice a year and, where necessary, at the duly reasoned request of the Commission or a Member State. It works closely with the European cooperation network on elections, the European Regulators Group for Audiovisual Media Services and other relevant networks or bodies, in order to facilitate the rapid and secure exchange of information on matters connected with monitoring and enforcement of this Regulation. The Commission participates in the meetings of the network and provides administrative assistance.	

9. A Member State designating more than one competent authority shall ensure that the respective tasks of those authorities are clearly established and that the authorities cooperate closely and effectively in carrying out their tasks. Each Member State shall designate one competent authority as the national contact point at Union level for all aspects of this Regulation. National contact points shall support and facilitate effective cooperation among national competent authorities and with the national contact points of other Member States. Member States shall make publicly available the contact details of their national contact points. The Member States concerned shall, where appropriate, communicate the names of the other competent authorities and their respective tasks to the network of national contact points.	
Article 24 Right to lodge a complaint	Every person has the right to lodge a complaint with the competent national authority,

1. Without prejudice to any other administrative procedure or judicial remedy, the competent authorities shall duly handle every notification of a possible infringement of this Regulation and, upon request, inform the person who made the notification of the follow-up given. During the last month preceding an election or referendum, any notification received in relation to that election or referendum shall be handled without undue delay. 2. The competent authorities shall transmit without undue delay complaints falling within the competence of another competent authority in another Member State to that competent authority.	which must handle every notification. During the last month preceding an election or referendum, any notification must be examined without undue delay.
Article 25 Sanctions 1. Member States shall lay down the rules on penalties or other necessary measures applicable to sponsors or political advertising service providers in the event of infringements of Articles 5 to 17, 20 and 21, and shall take all measures necessary to ensure their timely implementation. […] 5. Infringements of Articles 5, 7, 11, 12, 13, 15, 16 and 18 shall be considered particularly serious where they concern political advertising messages published or disseminated during the last month preceding an election or referendum and addressed to citizens of the Member State in which the election or referendum	As regards the sanctions to be applied, it is for Member States to lay down the relevant rules within the regulatory framework established by the European legislator. Certain infringements are automatically considered particularly serious where they concern political advertising messages published or disseminated during the last month preceding an election or referendum, given the

is organised. Member States may also impose periodic penalty payments to compel sponsors, political advertising service providers and political advertising publishers to bring a serious and repeated infringement of this Regulation to an end.	relevance of those rules for the protection of recipients' rights.

3 Artificial intelligence in the sectors regulated by AGCOM: mapping impacts and an operational framework for intervention

Andrea Imperiali

3.1 Introduction. Artificial intelligence as a cross-cutting paradigm

Artificial intelligence is not a technology that can be brought back within the categories of ordinary innovation. Its transformative reach, the speed with which it penetrates the visible and invisible processes that govern daily life, and the fundamental ambiguity of its impact place it in a wholly distinctive position in the contemporary regulatory landscape. AI can operate simultaneously as a silent enabler of efficiency, as a multiplier of pre-existing imbalances and as an opaque tool of manipulation. Above all, it is capable of cutting diagonally across sectors, competences, rights and languages, posing unprecedented challenges to any regulatory authority.

In this scenario, an independent authority such as AGCOM cannot confine itself to traditional sectoral analysis, nor can it wait for the national or European legislator to define a definitive regulatory perimeter which, in the case of artificial intelligence, is structurally likely to lag behind technological and market developments. From a legal-institutional standpoint, this implies the need for an anticipatory and adaptive approach, combining legal certainty with the flexibility of regulatory tools, in a context in which the very nature of the regulated object — autonomous algorithmic systems capable of learning and adapting — challenges traditional legal categories of liability, transparency and control.

3.1.1 The choice to start from areas of competence

The most common methodological approach to AI structures the analysis by industrial sectors (healthcare, education, transport, communications) or by technological types

(language models, predictive systems, personalised recommendations). Such mapping is useful, but not always sufficient for independent authorities, which operate not so much along the vertical lines of production sectors as along cross-cutting axes of guarantee: protection of fundamental rights, promotion of competition, supervision of service quality and information balance. The Committee therefore chose to organise the analysis into four fundamental blocks, each corresponding to one of the Authority's formal areas of competence: (i) electronic communications, (ii) digital services, audiovisual and radio media, (iii) postal services, and (iv) consumer and user protection. This choice, perhaps less elegant from a systematic point of view, is more consistent with AGCOM's institutional mission and anchors the analysis to what the Authority is already called upon to do every day: regulate, monitor and safeguard.

3.1.2 The distinction between actual and potential impacts

For each impact identified, the report specifies whether it is a phenomenon already under way (actual impact) or one reasonably foreseeable in the short to medium term (potential impact). In several cases, both qualifications coexist. This distinction is not merely classificatory, but operationally and methodologically relevant:

actual impacts require immediate responses and readily deployable tools. These are documented phenomena, supported by empirical evidence, established cases or decisions by national and international authorities;

potential impacts require anticipatory action, study, observation and preparation of regulatory tools. These are risks with a high probability of materialising in the short to medium term, whose management requires a vigilant and adaptive regulatory posture.

This gives rise to a dual prioritisation matrix: the first classifies impacts by time horizon (immediate: 0–12 months; medium term: 1–3 years; prospective: 3–5 years); the second cross-references the severity of the impact with the level of regulatory preparedness (regulatory gap), allowing intervention priorities to be classified into four levels: maximum urgency (serious impact with a high regulatory gap), high priority (medium-high impact with a significant gap), monitoring (manageable impact with partial coverage), and no immediate action (low impact or adequate coverage).

3.1.3 The analytical structure: ex ante, in itinere, ex post

For each identified impact, the analysis was structured along five axes: (a) a concise description of the impact, with its qualification as actual or potential; (b) prioritisation matrices (time classification and severity/regulatory-preparedness relationship); (c) ex ante activities (prevention and preparation); (d) in itinere activities (continuous supervision); and (e) ex post activities (correction and enforcement).

This temporal tripartition reflects the life cycle of an advanced and modern regulatory policy: prevent, supervise, correct. It is not a theoretical exercise, but a concrete simulation of how AGCOM could intervene when faced with each risk or use of AI affecting its competences. The objective is not, of course, to anticipate specific regulatory choices, but to provide the Authority with an analytical compass for navigating complexity, identifying the most urgent areas, emerging systemic risks and opportunities to strengthen AGCOM's institutional role in an increasingly AI-driven digital ecosystem.

Ex ante activities were further divided into four categories: codes of conduct and co-regulation; guidelines and regulations; possible authorisation or notification systems; and training and literacy activities. In itinere activities include: procedures and standards; specialist tools (monitoring, audits, simulations); technical laboratories (sandboxes, testbeds, observatories); and outsourced activities or technical-scientific partnerships. Ex post activities include: corrective obligations, transparency measures towards users, and reporting or accountability obligations.

3.1.4 Note for the reader on the scope of the recommendations

This contribution is deliberately drafted from a broad-spectrum perspective: while it uses AGCOM's formal areas of competence as the organising axis of the analysis, some of the policy implications identified and recommendations formulated go beyond the direct perimeter of the Authority's powers, touching on matters — such as antitrust rules, privacy protection and institutional governance of the AI Act — that fall within the competence of other national authorities, the legislator or the European Commission. This choice is conscious and methodologically justified: independent authorities operate not along the vertical axes of sectoral boundaries, but along the

horizontal axes of the protection of rights, pluralism and market balance; and an analytical mapping of AI cannot but reflect this cross-cutting vocation. The AGCOM Council, as recipient of this Report, will assess, in its autonomy, which recommendations to adopt as its own and which to transmit to the competent institutional fora.

3.2 Electronic communications

3.2.1 The impact framework

Artificial intelligence is profoundly transforming the electronic communications sector, with impacts affecting network-infrastructure management, data-traffic neutrality, competition between operators and user protection. The Committee identified twenty specific impacts in this area, four of which were classified as maximum urgency.

Dynamic network management. AI systems are already central to traffic optimisation, automated allocation of network resources and prediction of infrastructure failures. Through predictive models and real-time monitoring, AI improves the stability and resilience of services, with tangible benefits such as fewer outages and preventive maintenance. However, the progressive delegation of critical technical decisions to algorithms introduces significant risks requiring regulatory attention: unforeseen errors that may propagate at scale, vulnerabilities to cyber sabotage (adversarial attacks on predictive systems), and above all the progressive loss of human control over critical processes. The principle of human oversight, a cornerstone of the AI Act (Article 14), finds here one of its most significant applications.

Net neutrality and algorithmic discrimination in data traffic. One of the most relevant and urgent impacts concerns the risk that AI systems for traffic management may apply non-transparent discrimination between different flows. In practice, this takes specific and documented forms:

Dynamic zero rating: AI systems identify in real time the operator's commercial-partner services and exclude the related traffic from data consumption, thereby penalising competitors. The most significant Italian case concerned a mobile operator offering unlimited traffic for partner music-streaming services, while traffic towards competing services counted against data allowances.

Selective throttling: algorithmic reduction of speed for specific applications such as VoIP (WhatsApp calls, Skype) during peak hours, without transparency towards users, in order to encourage the use of traditional paid calls.

Commercial prioritisation: preferential bandwidth allocation to "premium" services (cloud gaming, enterprise videoconferencing) to the detriment of less profitable services such as information sites, small e-commerce services or digital public services. Independent tests such as Wehe App, Northeastern University have identified several cases of traffic differentiation and throttling on different mobile networks globally, although no consolidated public data with specific percentages for the Italian market are available.

The evidence collected shows that these practices are already occurring: between 2018 and 2023, AGCOM received several reports concerning suspected breaches of net neutrality, opening sanctioning proceedings, some of which ended with findings of infringement. Regulation (EU) 2015/2120 on Open Internet expressly prohibits blocking, throttling and commercial prioritisation (Article 3(3)), but the lack of automated testing tools, the adequacy of sanctions and the burden of proof on users make enforcement structurally weak.

Infrastructure impact of large AI models. The growth of generative AI services is significantly increasing network-capacity requirements at the level of data-centre interconnections and international peering, with projections indicating that by 2030 a substantial share of network traffic will involve AI processing (Omdia/Frontier Economics, 2024); the impact on consumer internet traffic remains more limited for text-based services, while becoming relevant for multimodal services (audio and generative video). The infrastructure implications are multiple: the need to anticipate capacity investments by 2–3 years compared with original plans; pressure on international peering agreements (EU-US data traffic for access to cloud models); and planning difficulties due to unpredictable usage patterns. The European debate on the so-called fair share — the request by major telecoms operators that leading traffic generators contribute to infrastructure costs — was relaunched in 2022–2023, but the Commission's public consultation (October 2023) recorded its rejection by the

majority of respondents and by the European Parliament (BEREC, Internet Society, 2023).

Edge computing and digital sovereignty. Processing data ever closer to the end user (edge computing) allows lower latency and better performance, but shifts the processing of personal information to distributed nodes, often outside national territory. AI distributed across thousands of edge nodes makes it complex to trace data flows, verify GDPR compliance and exercise data-subject rights. The risk is loss of control over the physical localisation of data, with implications for digital sovereignty, applicable jurisdiction and enforcement capacity.

Concentration of market power. Operators capable of developing proprietary AI algorithms and accessing massive datasets acquire competitive advantages that are difficult to close, creating new barriers to entry for competitors. The phenomenon operates through a vicious circle (flywheel effect): more data generate better algorithms, producing better services, attracting more customers and generating more data. Sector data are eloquent: in Italy, TIM, Vodafone (now merged into Fastweb+Vodafone) and WindTre control almost 80% of the mobile market; declared AI investments amount to several hundred million euro for 2023–2025, compared with a few tens of millions for challengers such as Iliad. At European level, AI-centric acquisitions in the telecoms sector grew significantly between 2020 and 2023, with almost all transactions below mandatory notification thresholds — a figure revealing the structural inadequacy of traditional antitrust tools for markets in which value lies in intangible assets (data, algorithms, know-how).

Dynamic pricing and algorithmic collusion. The use of algorithms that monitor competitors' pricing strategies in real time and automatically update tariffs may lead to tacit algorithmic collusion: price convergence towards supra-competitive levels without any explicit agreement between operators. The mechanism operates in four phases: monitoring (automatic price scraping), analysis (identification of optimal pricing through game theory and reinforcement learning), response (automatic adjustment), and collusive equilibrium (all algorithms converge towards the same pricing without communication). The French Autorité de la concurrence has documented cases of abnormal price convergence among mobile operators despite

reductions in infrastructure costs. Academic simulations (Calvano et al., 2020, American Economic Review) show that Q-learning algorithms, not programmed to collude, autonomously develop collusive strategies with systematically supra-competitive prices. The legal paradox is that Article 101 TFEU requires proof of "concertation", which is by definition absent in algorithmic collusion.

Dynamic management of radio spectrum. AI enables dynamic and predictive real-time allocation of frequencies, optimising the use of scarce spectrum. However, proprietary algorithms could favour certain operators or services, generate unforeseen interference or allocate resources in a discriminatory manner without transparency. The risk is loss of public control over a strategic resource, with possible breaches of the principles of fair access to spectrum and competitive distortions.

3.2.2 Intervention priorities and operational recommendations

The prioritisation matrix identifies six maximum-urgency impacts in the electronic communications sector: algorithmic breach of net neutrality, AI-driven concentration of market power, collusive dynamic pricing, AI-centric mergers, surveillance and privacy, and discriminatory traffic management. For each, the regulatory gap was assessed as high, requiring immediate regulatory interventions. The analytical sheets annexed to the report detail, for each maximum-urgency impact, operational recommendations with short-term (0–6 months), medium-term (6–18 months) and long-term (18–36 months) horizons, accompanied by monitoring indicators (KPIs) with baselines and targets.

Among the most urgent interventions, not all of direct AGCOM competence, are: adoption of automated tools for testing net neutrality (modelled on the Net Neutrality Reference Measurement System developed by BEREC and already adopted by BNetzA in Germany within the breitbandmessung.de service, available open-source on GitHub); introduction of prior-notification obligations for AI systems used in traffic management; assessment of tools that rebalance the burden of proof in cases of discrimination reports (the operator must demonstrate non-discrimination, rather than the user proving the breach); definition of market-power assessment criteria including possession of strategic datasets, proprietary AI capabilities and vertical integration between algorithms, infrastructure and services; creation of an automated

monitoring system for price parallelism with alerts in case of abnormal convergence; and establishment of a voluntary register of AI-centric acquisitions with incentives for notification (fast-track pre-clearance) and disincentives for omission (in-depth investigation in case of post-facto discovery).

3.3 Digital services, audiovisual and radio media

3.3.1 The impact framework

The digital-services and audiovisual-media sector is the one in which the impact of artificial intelligence assumes the most alarming dimensions, both because of the pervasiveness of the phenomena and because of their relevance for fundamental rights — freedom of expression, information pluralism, human dignity, protection of minors and copyright. The Committee identified thirty impacts in this area, four of which were classified as maximum urgency.

Deepfakes and the disinformation ecosystem. The automatic generation of audiovisual content — deepfake videos, voice synthesis, synthetic media — has reached levels of sophistication that make false content indistinguishable from authentic content for the vast majority of users. The empirical evidence is unequivocal: in the Slovak parliamentary elections of September 2023, a deepfake audio of a political leader raised concerns about a potential impact on the loss estimated in exit polls and even of a few seats in Parliament — and fact-checking took 18 hours to issue a denial, a timeframe incompatible with viral diffusion; in the 2024 US primaries, robocalls using President Biden's cloned voice invited voters not to vote; deepfake videos of candidates in compromising situations were circulated on X and TikTok. In Italy, during the 2024 European elections, AGCOM received several reports of possible deepfake content. The AI Act (Article 50(4)) provides for an obligation to label AI-generated or manipulated content "clearly and distinguishably", but the ambiguity of this wording, the absence of implementing technical standards (label format, position, language), limited detection capacity by authorities and the absence of rapid-response mechanisms make the current regulatory framework insufficient.

AI-powered search engines and the sustainability of journalism. The introduction of AI-powered features in search engines (Google AI Overview, Bing AI Mode,

Perplexity) radically changes user-information interaction: instead of providing links to external sources, these systems generate direct synthetic answers based on content extracted from the web. The shift produces multiple consequences: a drastic reduction in traffic towards editorial sites (with documented declines), directly affecting the economic sustainability of journalism and especially local journalism; information concentration through presentation of a "single answer" instead of a plurality of sources, thereby compromising users' exposure to different perspectives (even where those search engines indicate sources at the bottom); reuse of journalistic content without adequate compensation, potentially infringing Article 15 of the Copyright Directive; opacity regarding sources and synthesis methodology, with risk of disinformation if the AI misinterprets or extrapolates content out of context; and self-preferencing by dominant platforms that keep users within their services instead of redirecting them to the open web, raising issues under the Digital Markets Act.

Recommendation algorithms and pluralism. AI-optimised recommendation algorithms shape user preferences by creating "information bubbles" that limit exposure to different perspectives. Empirical data are significant: independent analyses (e.g. Mozilla Foundation) have shown that 71% of content received "regrettable" recommendations (violence, disinformation, conspiracy theories) and that many problematic recommendations involved content never searched for by users, proactively suggested by the algorithm. The DSA (Articles 34 and 38) requires VLOPs to assess systemic risks, including those arising from recommendation algorithms, and to offer users at least one option not based on profiling, but it does not precisely define standardised metrics and verifiable independent audits.

Copyright and model training. The mass use of protected audiovisual works for training generative models raises critical issues of fair compensation, authors' consent and traceability of content origin. It is widely recognised that datasets used to train large language models include a significant amount of copyright-protected content, often acquired through mass online data-scraping techniques. The possible use of protected works without adequate licensing or remuneration mechanisms is currently the subject of litigation and intense regulatory debate at European and international level, including in relation to sustainable compensation models for rights holders. In

Italy, bodies representing authors and publishers, including SIAE and AIE, have taken positions in the debate on the use of protected works by AI systems, calling for greater transparency, licensing mechanisms and forms of remuneration for rights holders. The Text and Data Mining exception under Article 4 of Directive (EU) 2019/790 allows the use of content, including for commercial purposes, unless rights holders have expressly opted out. However, in the context of generative AI models, application difficulties have emerged regarding systematic verification of such opt-outs in mass data collection. The AI Act introduces specific obligations for general-purpose models (GPAI), including publication of a summary of training data and measures for copyright compliance. However, the regulation does not directly address remuneration of rights holders, leaving open the need for further regulatory developments on licensing and compensation.

AI-driven advertising, advertising chatbots and commercial practices. The integration of conversational AI systems into digital marketing takes increasingly sophisticated and legally problematic forms. On the one hand, chatbots acting as brand influencers develop parasocial relationships to promote products; on the other, OpenAI announced for 2025 the inclusion of sponsored content in conversations with ChatGPT. These tools exploit conversational personalisation, real-time emotional analysis and behavioural adaptation to steer purchasing choices through interactions that appear neutral or assistive. Emerging risks include covert advertising disguised as personalised recommendations, behavioural manipulation through exploitation of psychological vulnerabilities, mass profiling without adequate informed consent, and targeting of minors and vulnerable persons. The mixture of assistive function and commercial purpose makes the advertising nature of the interaction opaque, circumventing disclosure requirements under rules on advertising transparency and unfair commercial practices, and potentially configuring forms of subliminal cognitive manipulation prohibited by Article 5 of the AI Act.

Electoral manipulation, par condicio and political micro-targeting. The recommendation and ranking algorithms of digital platforms may alter the visibility of candidates and parties in a non-transparent manner, undermining par condicio. The logic by which platforms display certain political content is often inscrutable:

candidates, political forces or minority ideas may be systematically penalised without any possibility of external verification. Political micro-targeting through predictive AI enables campaigns targeted at the individual level, exploiting psychographic profiling and user vulnerabilities — as demonstrated by the Cambridge Analytica precedent and its technological evolutions. Automatic production of synthetic political content (fake interviews, synthetic news, deepfake videos) is a concrete threat to the integrity of democratic processes. Law 28/2000 (par condicio), conceived in a predominantly television and radio media context, does not contemplate the dynamics of the digital ecosystem or the algorithmic dimension of political-content distribution and visibility.

Concentration of the supply chain in the hands of AI-owned platforms. Major technology platforms increasingly integrate different components of the digital supply chain, including AI-system development, infrastructure management and control of content-distribution channels. This integration strengthens dynamics of market-power concentration, already recognised at European level through the gatekeeper rules, and may favour self-preferencing practices, affecting market-access conditions for third-party operators and the distribution of economic value between platforms and content creators. Moreover, the central role of algorithmic recommendation systems allows platforms to influence significantly the visibility and circulation of information in public debate. In this context, traditional antitrust measures, designed for industrial markets, show limits when applied to business models based on data, algorithms and platform dynamics, as highlighted by the evolution of the European regulatory framework.

3.3.2 Intervention priorities and operational recommendations

The sector records four maximum-urgency impacts and six high-priority impacts: deepfakes and disinformation, AI electoral manipulation, copyright infringement through training, political micro-targeting, opacity of political-content ranking and proprietary concentration of AI-owned platforms. The operational recommendations, again not all directly and exclusively attributable to AGCOM, include: expanding and strengthening the electoral par condicio task force, with 24/7 operational capacity during campaigns (composed of AGCOM, the Postal Police and platform representatives); defining protocols with major platforms for rapid removal of political

deepfakes (within two hours of reporting); defining implementation standards for labelling AI-generated content under Article 50 of the AI Act (format, positioning, language); acquiring or developing forensic deepfake-detection capacity (partnerships with Politecnico di Milano, FBK Trento, or commercial software such as Sensity and Reality Defender); launching a roundtable with SIAE, the Ministry of Culture and the Data Protection Authority for an Italian licensing and fair-compensation framework; promoting cryptographic watermarking standards (C2PA, Content Authenticity Initiative) for content authenticity; and a legislative proposal to assess the opportunity to introduce specific provisions for an electoral deepfake offence with aggravated penalties and reversal of the burden of proof in civil proceedings.

3.4 Postal services

3.4.1 The impact framework

Although the postal sector presents moderate complexity compared with the previous sectors (two high priorities out of eight impacts identified), artificial intelligence produces significant impacts there, with important implications for territorial cohesion, social inclusion and financial inclusion.

Logistics optimisation and territorial gaps. AI systems for sorting, routing and delivery forecasting improve operational efficiency, but structurally tend to privilege economic profitability (cost/delivery, shipment density/km^2), systematically penalising low-density areas, municipalities with older populations and smaller islands. Poste Italiane data document significant reductions in physical access points and service hours in rural, mountain and southern areas. In recent years, monitoring activities and reports received by the Authority and other institutional actors have highlighted critical issues in the quality and continuity of the universal postal service, particularly in certain territories. In this context, the introduction of advanced operational-optimisation tools, including algorithmic systems, raises a significant regulatory issue concerning the balance between efficiency objectives and universal-service obligations. This profile directly recalls the founding principles of postal regulation, as defined by Directive 97/67/EC and Legislative Decree 261/1999.

Postal financial services and algorithmic discrimination. Postal operators provide financial services (BancoPosta, PostePay, loans, investments) that integrate AI for credit scoring, automated advice (robo-advisory) and fraud detection. The risk is algorithmic discrimination: models trained on historical data reflecting socioeconomic, geographical and age-related biases may systematically penalise women, young people, residents in disadvantaged areas and precarious workers. Lack of transparency in decision criteria prevents users from challenging refusals and verifying the fairness of decisions, in breach of equal-treatment and consumer-protection principles. The AI Act classifies creditworthiness assessment systems (credit scoring) as high-risk systems (Article 6 and Annex III, point 5(b)), imposing obligations on risk management, data quality and bias mitigation, transparency, human oversight and system robustness. The enforcement system is, however, being progressively implemented and will require development of technical standards, as well as strengthening of supervisory capacity and coordination between competent authorities.

Green logistics and algorithmic greenwashing. AI systems for optimising delivery routes can reduce emissions and waste, but the emerging risk is algorithmic greenwashing: operators claim emission reductions based on unverifiable AI models, with little transparency on data, methodologies and actual results. Without independent measurement standards, audits and credible certifications, AI-based sustainability promises risk becoming misleading marketing.

Blockchain+AI traceability. The integration of blockchain and AI promises end-to-end traceability of shipments and anti-counterfeiting measures, but raises issues of commercial surveillance: every movement of goods, and indirectly of people, is monitored, profiled and analysed for commercial purposes, with risks of profiling purchasing habits and possible discrimination against suppliers or customers.

3.4.2 Intervention priorities

The mapping suggests: introducing explicit constraints in logistics-optimisation algorithms that guarantee minimum universal-service standards irrespective of profitability; defining non-derogable territorial-accessibility KPIs, with periodic audits; adopting explainability and anti-discrimination audit obligations for postal

credit-scoring systems, with the user's right to a detailed statement of reasons for refusals and to human review; and defining environmental-reporting standards for AI-driven green-logistics claims, with independent certification and sanctions for established greenwashing.

3.5 Consumer and user protection

3.5.1 The impact framework

Consumer and user protection is the sector with the highest criticality: the mapping identifies as many as four maximum-urgency impacts out of fourteen overall impacts, with risks directly affecting the fundamental rights of the person.

Opaque automated decisions. A user may receive a decision — acceptance or rejection of a refund, contract modification, application of penalties, personalised offer — without any possibility of understanding the underlying logic or challenging the outcome. The right not to be subject to decisions based solely on automated processing with legal or similarly significant effects, enshrined in Article 22 GDPR, presents significant application difficulties in practice. In particular, operators may rely on exceptions provided for by the Regulation, including those linked to contractual necessity, while the ways of exercising rights and challenging decisions are often complex or insufficiently transparent for users. Moreover, the average user may have difficulty identifying and understanding automated decisions and effectively activating protection mechanisms. The AI Act introduces complementary obligations, especially on transparency and technical documentation for high-risk systems, but significant challenges remain in terms of enforcement and supervisory capacity.

Biometric surveillance. AI systems for biometric identification — facial recognition, voice recognition, gait analysis, behavioural biometrics — are already widely used by telecom operators, service providers and platforms for network security, customer authentication and cooperation with law enforcement. The Clearview AI case (2022), concluded with a fine of 20 million euro by the Italian Data Protection Authority for the use of facial-recognition systems based on mass scraping of online images, is an emblematic example of the risks associated with biometric data. A further risk profile is function creep, namely reuse of biometric data collected for specific purposes (e.g.

authentication) for further purposes such as marketing or profiling, without an adequate legal basis. The AI Act prohibits certain practices, including social scoring (Article 5(1)(c)) and biometric categorisation intended to infer sensitive characteristics (Article 5(1)(d)), as well as real-time remote biometric identification in public spaces, except for specific law-enforcement purposes relating to serious crimes. The breadth and complexity of the conditions for such exceptions have raised questions about the risk of expansive applications, while effective enforcement of the prohibitions will require significant strengthening of supervisory capacities.

Cognitive manipulation of vulnerable persons. Adaptive interfaces and predictive systems that exploit psychological vulnerabilities can induce non-conscious behaviours, especially among minors and fragile persons: social-media addiction (addiction by design), purchase traps, extreme polarisation of opinions. The AI Act prohibits subliminal cognitive manipulation causing significant harm (Article 5(1)(a)), but so-called AI-powered dark patterns — interface design using AI to exploit cognitive vulnerabilities and steer user choices — occupy a regulatory grey area. In Italy, about 45–46% of the population aged 16 to 74 has at least basic digital skills (Eurostat). Significant gaps also remain by age, level of education and territorial context, particularly in the South and inland areas.

AI in ADR systems and legaltech. The integration of AI into alternative dispute-resolution systems (ODR) to analyse complaints, propose solutions and mediate between parties presents risks of pro-company bias (models trained on decision histories favouring the enterprise), lack of personalisation for complex cases and compression of procedural guarantees. At the same time, the spread of automated legal-assistance tools (legaltech), including legal chatbots, can facilitate access to basic legal information and help reduce economic and informational barriers. However, such tools may involve risks of incorrect or incomplete legal information, difficulty in adapting answers to the specific circumstances of a case and uncertainty as to liability for the indications provided. In this context, the distinction between generic legal information, generally admissible, and personalised advice, reserved to qualified professionals, becomes particularly important, requiring clarification, also at

regulatory level, of the boundaries between the two categories and their respective liability regimes.

Algorithmic discrimination in insurance and credit. The insurance and credit sectors make massive use of AI to assess risks (underwriting), calculate personalised premiums (pricing) and manage claims (claims processing). Academic and institutional literature documents how algorithmic systems may produce discriminatory effects, including indirect effects, against specific groups in relation to characteristics such as gender, ethnic origin, socioeconomic conditions or health status. These effects may emerge even without explicit use of sensitive data, through apparently neutral variables (proxies), such as geographical location, digital behaviour or other indirect indicators statistically correlated with protected characteristics.

This phenomenon raises significant issues from the standpoint of non-discrimination and user protection, requiring adequate tools for assessment, transparency and control of algorithmic systems. Predictive profiling risks transforming statistical probability into individual destiny, crystallising and amplifying existing inequalities.

3.5.2 Intervention priorities

The four maximum-urgency impacts — opaque automated decisions, biometric surveillance, cognitive manipulation of vulnerable persons and deepfakes causing individual harm — require immediate and structural interventions. The recommendations are: adoption of explainability obligations for all automated decisions; a guaranteed right to human review on request; establishment of a centralised helpdesk for consumer reports relating to automated decisions, integrated with existing user-protection and complaint-handling mechanisms; a moratorium on the use of facial recognition for purposes other than 1-to-1 authentication; formal coordination protocols with the Data Protection Authority, AGCM, Banca d'Italia and IVASS for joint audits; recognition that the growing use of synthetic-content generation techniques has fuelled debate on the possible introduction of specific provisions on non-consensual deepfakes, also with reference to strengthening victim-protection tools. At the same time, the European framework — in particular the Digital Services Act — introduces prohibitions on dark patterns and provides specific protections for minors. The evolution of AI systems, including those capable of personalising and

optimising interactions with users, nevertheless makes further development of regulatory tools necessary to prevent manipulative practices.

3.6 Conclusions: towards an integrated operational strategy

3.6.1 Cross-cutting synthesis of priorities

The cross-cutting analysis of the four areas of competence reveals several maximum-urgency impacts with cross-sectoral relevance. The following list is not merely a catalogue but an operational hierarchy: each item reflects the combination of impact severity, breadth of regulatory gap, cross-cutting relevance to AGCOM's areas of competence and temporal urgency of intervention.

AI electoral manipulation (Media, Consumer protection) — requires guidelines for algorithmic par condicio in the digital environment and mandatory labelling of AI-generated political content. The urgency is maximum in view of the next Italian political elections (2027): without an operational protocol activated with platforms, the risk of an "Italian Slovakia case" is concrete.

Deepfakes and disinformation (Media, Consumer protection) — require an integrated framework for detection, transparency on content origin and rapid response. The time between the spread of a deepfake and its debunking (currently estimated at 18 hours in the best case) is incompatible with digital-information cycles.

Breach of algorithmic net neutrality (Telecommunications) — the evolution of traffic and network-management systems, increasingly based on automated and algorithmic logic, raises new questions regarding application of the net-neutrality principle. In this context, there may be a need to extend monitoring and verification tools to algorithmic traffic-management methods, through development of adequate technical standards and stronger enforcement mechanisms. Technical tools developed within BEREC and by certain national authorities already allow monitoring of specific aspects of net neutrality and could provide a basis for further evolutionary developments.

Non-transparent automated decisions (Telecommunications, Postal services, Consumer protection) — require mandatory explainability, the right to human appeal

and an accessible reporting system. This is the most cross-cutting impact: from telecom customer care to postal credit scoring, from content moderation to ADR procedures.

AI-driven concentration of market power (Telecommunications, Media) — the growing concentration of market power in the telecoms and digital-media sectors is further strengthened by intensive use of data and algorithmic systems. In this context, the need emerges to evolve antitrust-analysis tools, also in order to consider the role of data and algorithms in determining market power, and to strengthen mechanisms such as data portability to reduce barriers to platform switching for users. Moreover, the inadequacy of traditional merger-notification thresholds, based mainly on turnover, is one of the main critical issues highlighted in the European debate on digital markets.

Biometric surveillance (Telecommunications, Consumer protection) — requires a moratorium on facial recognition in commercial public spaces, mandatory DPIAs for biometric systems and formal notification to the authorities. The intersection between DPI (Deep Packet Inspection) and AI analytics represents the most insidious form of potential hidden surveillance.

Algorithmic collusive pricing (Telecommunications) — requires detection tools, a regulatory sandbox for pricing algorithms and revision of antitrust evidentiary tools. The structural impossibility of proving an "agreement" in algorithmic collusion makes it necessary to introduce new approaches to legal presumptions.

Copyright infringement through training (Media) — the use of copyright-protected content in the training of artificial-intelligence models raises significant legal issues, currently the subject of litigation and debate at European and international level.

In this context, proposals have been put forward for the introduction of tools such as training-dataset registers, collective licensing models and compensation mechanisms for rights holders. The Text and Data Mining exception under Article 4 of Directive (EU) 2019/790, which allows the use of content unless rights holders opt out, is subject to controversial interpretations, also in light of mass data-collection methods in generative AI systems, and may require further regulatory and application guidance at European and national level.

Cognitive manipulation of vulnerable persons (Media, Consumer protection) — AI systems may be used to influence user behaviour, with particularly significant risks for vulnerable persons, including minors. In this context, there is a need to strengthen measures against manipulative practices, including so-called dark patterns, also in light of the growing use of advanced algorithmic techniques, and to develop effective child-protection tools, such as age-verification mechanisms and limits on persuasive techniques. The AI Act (Article 5) introduces prohibitions relating to manipulative practices and exploitation of vulnerabilities, but their practical application raises interpretative questions, particularly regarding definition and identification of subliminal manipulation techniques.

Systemic discriminatory bias (all areas) — requires algorithmic auditing and a fairness-by-design approach as a compliance requirement. It is the only impact crossing all four AGCOM areas of competence.

3.6.2 Ex ante activities: preventing, preparing, enabling

On the prevention front, the analysis delivers a clear message: the ex ante phase is not a merely technical-preparatory exercise, but an act of institutional positioning requiring robust choices and strategic vision.

Codes of conduct and co-regulation are the most recurring tool in the operational recommendations and the one with greatest flexibility. They ensure adaptability (they can be updated more frequently than legislation), ownership by regulated entities (which participate in their definition) and institutional legitimacy (they are adopted or approved by the Authority). However, they must be designed with a cross-sectoral vision: multiplying codes for each sector (one for customer care, one for media, one for advertising) could be counterproductive. The report raises — leaving open for reflection — the question of whether a single AGCOM Code for responsible use of artificial intelligence in regulated sectors should be adopted, with modular specific sections but common principles (transparency, human oversight, non-discrimination, protection of vulnerable persons).

Technical guidelines and regulations should be adopted urgently in the most exposed sectors: guidelines and technical regulations appear particularly appropriate in the most exposed sectors. In algorithmic recommendation, the European framework

already requires, for very large platforms, at least one non-profiling-based option, but leaves open the definition of more precise metrics on pluralism and content diversity. For AI-generated content, the implementation of the European framework may require more detailed standards on labelling and traceability. For dynamic pricing, EU law already imposes transparency where personalisation is based on automated decisions, while possible developments on more granular disclosure remain open. Similarly, for advertising transparency and child protection, the DSA already provides a relevant basis, but the growing use of chatbots and AI assistants may require further application specifications.

The possibility of authorisations and notifications emerges as a tool to be adopted in the future for specific high-risk cases: AI in decision-making postal services (credit scoring, complaint handling), AI in political content (during electoral periods), AI in discriminatory data-traffic management (traffic management, zero rating), and AI in biometric surveillance (facial recognition, behavioural analysis). The notification framework must be light — so as not to paralyse innovation or deter investment — but sufficiently clear regarding boundaries that cannot be crossed and the consequences of failing to notify.

Training and literacy are a fundamental and often overlooked safeguard, operating on three distinct levels: (a) AGCOM internal resources, with structured training programmes on the AI Act, risk assessment, algorithmic audit, explainability and deepfake detection, aimed at both technical and legal-administrative staff; (b) operators and stakeholders, with workshops, practical guidelines and FAQs on compliance obligations, responsible use of AI and best practices; and (c) end users and citizens, with media and digital literacy campaigns on recognising AI-generated content, digital rights and ways to report abuses or discrimination.

3.6.3 In itinere activities: supervising while everything evolves

AI is dynamic by definition: models learn, datasets change and applications evolve. Continuous supervision cannot be based exclusively on ex post logic (intervention after a report or harm) and requires specific tools, different from those used for supervision of traditional services.

Supervisory procedures and standards. It is essential to define a common minimum standard for auditing AI systems, applicable across sectors and also in cooperation with other authorities. Procedures must enable not only information recording, but also rapid intervention. The report suggests adopting an AI audit protocol structured in four phases: (1) notification and information collection; (2) technical analysis of the system (documentation, testing, simulations); (3) regulatory compliance assessment (AI Act, DSA, EECC, GDPR); and (4) operational measures (corrective measures, adjustment obligations).

Specialist tools. This area represents one of the most significant strategic investments for the evolution of the Authority's operational capacities. In particular, the Authority should equip itself with advanced technical tools for: monitoring algorithmic recommendation systems (analysis of diversity, bias and polarisation); forensic detection of synthetic content (audio, video and image deepfakes); analysis of bias and discrimination in automated systems (e.g. scoring, pricing, content moderation); tracking and verifying transparency of advertising content, including content generated or conveyed through AI systems; analysis of emerging market dynamics, including algorithmic-pricing scenarios and possible collusive behaviours; and testing net neutrality (traffic simulations, QoS analysis, detection of discriminatory practices). Tools developed at European level (e.g. BEREC, ERGA) may provide a methodological reference basis, while solutions already adopted by other national authorities, including the Bundesnetzagentur, could be assessed for possible adaptation. For specific areas such as detection of synthetic content, both partnerships with national universities and research centres (e.g. Politecnico di Milano, FBK, CNR) and adoption of technological solutions available on the market appear feasible in the short term.

Technical laboratories and testing environments. In light of the increasing complexity of artificial-intelligence systems, the need emerges to strengthen the Authority's internal technical capacities through structured analysis and experimentation environments. From this perspective, it appears appropriate to develop capacities along two main lines: an AI & Media area, oriented towards testing recommendation systems, assessing algorithmic pluralism, detecting synthetic content (deepfakes) and analysing automated-moderation systems; and an AI & Regulation

area, aimed at simulating impact scenarios, developing predictive tools, analysing market behaviours and assessing automated pricing systems. These capacities should be developed in coordination with universities, research bodies, other authorities and centres of excellence, at national and international level, with a view to sharing knowledge and strengthening skills.

Technical-scientific outsourcing. Some functions may be delegated in a controlled manner: specific technical audits, impact assessments on complex systems, large-scale simulations, algorithmic stress tests. The report suggests creating an accredited register of third parties, with clear criteria of transparency, independence (absence of conflicts of interest with regulated entities), certified technical competence and accountability.

3.6.4 Ex post activities: intervening, correcting, making visible

Corrective measures. Corrective measures should be assessed case by case, according to a proportionate, modular and progressive approach, primarily oriented towards risk mitigation and system adaptation. In this context, interventions may include, depending on the case: modification of algorithmic systems, strengthening of transparency and comprehensibility obligations regarding operating criteria, reintroduction or enhancement of human supervision, and imposition of adjustment obligations within defined deadlines. In cases of serious and imminent risk to users or the public interest, more incisive measures may also be adopted, up to suspension of the service.

Transparency towards users. In many areas — advertising, customer care, recommendation, content moderation — transparency is the first and most effective form of protection. The report identifies a minimum set of necessary and immediately implementable obligations: automated disclosure ("you are interacting with an artificial-intelligence system"), visible and understandable labels on AI-generated content ("this content has been generated/modified with artificial intelligence"), clear notices when the interaction is with an automated system and not with a human operator, and proactive information on user rights (right to request human review, right to know the logic of the decision, right to complain).

Public reporting. Public reporting can be enhanced as a tool of accountability and benchmarking, helping to strengthen transparency and the effectiveness of regulatory action. From this perspective, the establishment of an annual AGCOM Report on artificial intelligence in regulated sectors is proposed, integrating quantitative data (e.g. number of reports, audits conducted, infringements found, sanctions imposed) and qualitative analysis (emerging trends, case studies, best practices). The report could also include an assessment of corrective measures adopted and their outcomes, and formulate systemic recommendations addressed to the legislator and the Government.

Sanctions. The adequacy of the sanctioning system is an essential element for the overall effectiveness of the regulatory framework, as it directly affects the capacity to ensure an adequate level of deterrence. In this context, sanctioning regimes under relevant national legislation may in some cases present limits in terms of sanction levels, especially in relation to large operators and data-intensive business models. The European framework introduces significantly higher sanctioning levels: the Digital Services Act provides for sanctions of up to 6% of annual global turnover (Article 52), while the AI Act establishes sanctions of up to 7% of global turnover for the most serious infringements (Article 99), and up to 3% for other types of infringement. From this perspective, it is important to ensure effective coordination between the different sanctioning regimes, guaranteeing proportionality, coherence and deterrent capacity.

3.6.5 Few tools, well designed

The cross-cutting mapping shows that many tools recur across multiple areas. They need not be multiplied: they must be designed once, carefully, and made adaptable to all uses. In particular, three axes appear indispensable:

1. A **modular regulatory framework**, with codes of conduct, guidelines and transparency obligations harmonised across sectors, based on common principles (transparency, human oversight, non-discrimination, protection of vulnerable persons) translated into specific operational obligations for each context;
2. A **modern technical-operational capability**, with AI-based tools, internal laboratories, scientific partnerships and accredited external collaborations, capable of evolving with the technology;

3. An **integrated regulatory-reaction capacity**, combining transparency towards users, modular corrective obligations, proportionate and deterrent sanctions, and institutional cooperation with other national and European authorities.

3.7 European regulatory benchmarks

AGCOM operates within a European regulatory ecosystem characterised by a growing level of coordination between national authorities and supranational bodies. In this context, comparative analysis of the experiences of other regulators — including Ofcom (United Kingdom), Arcom (France), Bundesnetzagentur (Germany), as well as the European networks BEREC and ERGA — highlights common evolutionary directions in the approach to regulation of artificial-intelligence systems in communications, media and digital services. In particular, these experiences show: progressive strengthening of the authorities' internal technical capacities; development of analysis and experimentation environments (labs, sandboxes, data-science units); increasing attention to algorithmic recommendation systems, synthetic content (deepfakes) and risks to information pluralism; recourse to structured cooperation with universities, research centres and other authorities; and integration between traditional regulatory tools and data-driven and risk-based approaches. These elements provide a useful reference for the evolution of the Authority's operational capacities.

3.7.1 Ofcom (United Kingdom)

Ofcom is one of the most advanced cases in Europe in integrating technological expertise into the regulatory function. The authority has progressively strengthened its internal capacities in digital and artificial-intelligence matters, including through specialised teams and structures dedicated to analysis of emerging technologies (Ofcom, Approach to AI, 2025; Ofcom Annual Plan). In particular, Ofcom: has developed an explicit strategy on the use and regulation of artificial intelligence (Ofcom, Supporting and harnessing AI innovation safely, 2025); has advanced internal expertise in data science and AI (Ofcom Annual Report; Ofcom statements on in-house technology expertise); has established testing and technology-analysis environments, including a Technology Lab within the Online Safety regime (Ofcom, Online Safety

regime implementation); and collaborates with academic institutions and research centres, including the Alan Turing Institute (Ofcom in collaboration with the Alan Turing Institute on safety technology taxonomy). The approach adopted is characterised by: a combination of innovation promotion and risk management (Ofcom, Approach to AI, 2025); progressive strengthening of transparency and accountability tools, in line with the Digital Services Act (Regulation (EU) 2022/2065); and significant investment in the authority's technical capacities. Lessons for AGCOM: a risk-based approach requires major investment in internal technical expertise; the ability to analyse complex systems is a necessary condition for effective enforcement.

3.7.2 Arcom (France)

Arcom, established in 2022 by the merger of CSA and HADOPI, represents a model of integration between audiovisual, digital and content-protection competences (Ordonnance No. 2021-580; Arcom Annual Report 2024). The authority has progressively developed: monitoring of digital services and online platforms, also in implementation of the Digital Services Act (Arcom reports on online platforms and intermediary services); tools for analysing content and information phenomena (Arcom studies on media pluralism and information integrity); and cooperation initiatives with institutional actors and private operators, particularly in the electoral field and in countering disinformation (Arcom electoral recommendations and guidance to platforms). The French model is characterised by: strong attention to information pluralism and cultural diversity (Arcom Annual Report; CSA audiovisual-regulation legacy); an approach oriented towards platform transparency, in line with the DSA; and use of both regulatory and cooperative tools (dialogue with platforms, recommendations, guidelines). Lessons for AGCOM: continuous and structured monitoring of digital phenomena is more effective than sporadic interventions; cooperation with platforms can be useful, but requires a solid regulatory framework.

3.7.3 BNetzA (Germany)

The Bundesnetzagentur (BNetzA) has developed a particularly advanced approach in the technical regulation of communications infrastructure, especially with regard to net neutrality and user protection (Bundesnetzagentur net neutrality framework;

Regulation (EU) 2015/2120). In particular, it actively participates in developing European methodologies within BEREC (BEREC Guidelines on Net Neutrality); uses technical tools to monitor service quality and traffic neutrality (Bundesnetzagentur broadband measurement tools; BEREC net-neutrality measurement methodologies); and has developed systems for collecting user reports (Bundesnetzagentur consumer complaint and reporting systems). The German model highlights the importance of independent measurement tools for operators' performance and behaviour; integration between technical analysis and supervisory activity; and the use of data and reports to identify systemic criticalities. Lessons for AGCOM: independent technical testing is an essential element of regulation; operators' declarations must be complemented by autonomous verification tools.

3.7.4 BEREC and ERGA

At European level, regulatory networks play a growing role in developing common approaches. BEREC has analysed the impact of artificial intelligence in the telecommunications sector (BEREC Report BoR (23) 93), highlighting: the increasing spread of AI solutions in networks and services; implications for regulation, particularly in transparency and net neutrality; and the need to develop adequate tools and competences for auditing systems. ERGA has instead focused on: the impact of algorithmic systems on information pluralism; dissemination of synthetic content (deepfakes); and protection of minors and vulnerable users (ERGA reports and statements on disinformation, media pluralism and platform regulation). Both networks are contributing to the development of shared methodologies, guidelines and recommendations, and coordination spaces among national authorities (BEREC Work Programme; ERGA annual reports). Lessons for AGCOM: active participation in European networks is essential to contribute to the definition of future standards and to strengthen the coherence of regulatory action at EU level.

3.7.5 Operational lessons for AGCOM

The comparative analysis highlights several relevant operational lessons:

Strengthening internal technical capacities is an essential enabling factor: the availability of specialist skills (data science, AI systems engineering, algorithmic auditing) reduces information asymmetry vis-à-vis regulated entities.

Independent and automated testing is a fundamental element of supervisory activity: integration between technical tools and regulatory analysis strengthens enforcement effectiveness.

Continuous monitoring of digital systems can be particularly effective compared with interventions based exclusively on periodic checks, especially in contexts characterised by high dynamism and adaptiveness of artificial-intelligence systems.

Forms of cooperation with platforms are effective when embedded in a clear regulatory framework and supported by credible enforcement tools capable of ensuring compliance with commitments undertaken.

International cooperation is indispensable, given the cross-border nature of AI-related phenomena, including dissemination of synthetic content, risks of algorithmic discrimination and digital-market dynamics.

3.8 Normative connection: the European legal mosaic

3.8.1 The cornerstone of the AI Act

Regulation (EU) 2024/1689 (AI Act), adopted on 13 June 2024 and generally applicable from 2 August 2026, with progressive application of some provisions until 2 August 2027, is the main reference point of the European legal framework on artificial intelligence. Its risk-based architecture distinguishes between prohibited practices (Article 5), high-risk systems (Article 6 and Annex III), systems subject to specific transparency obligations (Article 50) and systems generally not subject to additional specific obligations. For AGCOM, the Regulation's relevance is potentially high and cross-cutting, without prejudice to the fact that designation of national competent authorities is left to Member States under Article 70. In the electronic-communications sector, certain AI systems used in managing critical digital infrastructures could fall within high-risk systems, particularly where they perform the function of safety components under Annex III, point 2. In that case, the Title III obligations on risk management, data governance, technical documentation, record-

keeping, transparency and human oversight would apply. For such systems, the registration regime under Article 49 must be read in light of the specific features of Annex III, including the fact that systems under point 2 are registered nationally. The intersection with the European Electronic Communications Code is operational: the provisions on network and service security, service availability and access to emergency services (Articles 108–109 EECC) impose constraints that must remain compatible with the use of AI systems in network management. Similarly, the principle of net neutrality interacts with the transparency and control requirements of automated systems.

3.8.2 The DSA–AI Act intersection

AGCOM, as Digital Services Coordinator (DSC) for Italy, already exercises functions that have significant points of contact with the framework outlined by the AI Act. The DSA imposes on very large online platforms (VLOPs) and very large online search engines (VLOSEs) obligations to assess systemic risks (Article 34), including the operation of algorithmic systems, particularly recommendation systems, and their possible effects on disinformation, civic debate, electoral processes, public health and protection of minors; annual independent audit obligations (Article 37); and the obligation to offer at least one recommendation option not based on profiling (Article 38). In this context, a significant area of coordination between the two regimes emerges, useful to avoid duplication and promote integrated supervision. This convergence is particularly evident on at least three fronts: the DSA requires assessment of systemic risks also arising from algorithmic systems, while the AI Act introduces transparency obligations for specific types of synthetic content, including deepfakes; the DSA requires transparency for users on the main parameters of recommendation systems, while the AI Act imposes documentation and transparency obligations towards competent authorities; and the DSA prohibits dark patterns (Article 25), while the AI Act prohibits specific subliminal or manipulative practices significantly affecting people's decision-making autonomy (Article 5(1)(a)).

3.8.3 DMA, Copyright Directive and ePrivacy

The Digital Markets Act (Regulation (EU) 2022/1925), although not falling within AGCOM's direct competences, significantly affects the digital ecosystem in which the Authority operates. Gatekeepers designated by the Commission control a plurality of core platform services — including search engines, app stores, messaging services and social platforms — with significant effects on competitive dynamics and the distribution of digital content. In particular, data-portability obligations (Article 6(9)) and interoperability obligations for number-independent interpersonal communications services (Article 7) constitute important reference points for the evolution of the European regulatory framework on opening digital markets.

The Copyright Directive (EU) 2019/790, and in particular Article 4 on text and data mining, raises open questions regarding commercial training of artificial-intelligence models on protected works. The provision allows text and data mining also for commercial purposes, unless rights holders have expressly reserved such use appropriately, including through machine-readable means for online content. In this context, significant application difficulties remain, including in relation to verifying opt-outs in mass data collection, while the current framework does not provide a general compensation mechanism for rights holders. This fuels the debate on the desirability of further regulatory or contractual developments, including collective licensing and transparency on training datasets.

The ePrivacy Directive (2002/58/EC) also remains relevant with regard to techniques for analysing traffic and communications, including deep packet inspection. Article 5 protects the confidentiality of communications and traffic data and in principle prohibits interception or surveillance by persons other than users, except with consent or a specific legal basis. Consequently, deep packet inspection practices combined with analytics or profiling may raise significant issues regarding confidentiality of communications, except where strictly necessary for service transmission or otherwise justified under the applicable legal framework.

3.8.4 An operational framework for navigating complexity

The report proposes an operational framework structured on four levels for navigating complexity and the legal mosaic:

- **AGCOM as a natural hub** between DSA, AI Act, EECC and TUSMA, enhancing the concentration of competences already present within the Authority and promoting coherent, non-duplicative enforcement;
- **coordination protocols with other competent authorities and institutions**, including the Data Protection Authority (GDPR, ePrivacy, data governance), AGCM (competition, DMA, algorithmic collusion), the Ministry of Culture and representative bodies of rights holders (copyright and licensing of training data), as well as Banca d'Italia and IVASS (AI credit scoring and insurance);
- **intersectoral technical roundtables**, for example on AI & Telecommunications (AGCOM, ENISA, operators), AI & Media (AGCOM, broadcasters, platforms, fact-checkers, EDMO), AI & Consumers (AGCOM, consumer associations, Data Protection Authority, AGCM);
- **capacity building**, through strengthening specialist internal technical skills, broad AI training programmes for the Authority's offices, agreements with universities and research centres for technical support in system audits, and structured forms of cooperation with other European regulators.

3.9 Implications for the Italian legal framework

3.9.1 The five urgencies for jurists and policymakers

The Committee's analysis highlights a significant gap between the speed of adoption of artificial-intelligence systems in regulated sectors and the capacity of the current regulatory framework to address emerging risks. While the AI Act and the Digital Services Act provide a European reference architecture, their effectiveness will depend largely on the quality of national implementation and on the capacity of competent authorities to equip themselves with the technical, organisational and skills-based tools needed to ensure effective enforcement. In this context, five particularly relevant areas emerge.

First. The full operation of the competent authorities under Article 70 of the AI Act requires institutional clarity — in terms of allocation of competences, powers and resources — and adequate operational capacity. In this framework, if AgID and ACN are involved mainly in aspects relating to the design of solutions, under the DSA AGCOM will be involved in competence profiles relating to service issues.

Second. Coordination between national and European sanctioning regimes is a central issue. Sanctions under the national framework may be limited compared with the economic scale of digital operators, while European regimes (DSA and AI Act) introduce significantly higher sanctioning levels. This requires clear application mechanisms and possible regulatory coordination.

Third. The emergence of algorithmic-collusion phenomena poses new challenges for traditional antitrust tools. The current framework, based on the concepts of agreement and concerted practice, may require interpretative adaptations or regulatory evolution to address tacit coordination dynamics mediated by algorithmic systems.

Fourth. Copyright protection in the age of generative AI raises significant application difficulties, particularly concerning the use of protected works in training processes. The current framework, based on the TDM exception with opt-out, fuels debate on the desirability of further regulatory developments or market solutions, including licensing and transparency on datasets.

Fifth. Protection of vulnerable persons — including minors, older people and people with low digital literacy — requires strengthening existing tools and assessing the adequacy of current measures, including with regard to manipulative practices, interface transparency and digital literacy.

3.9.2 The challenge of proportionality and innovation

The report is aware of the risk of overly burdensome regulation that could slow innovation without producing effective safeguards. The proposed approach is based on three principles:

– **modularity**, understood as adoption of tools adaptable to different contexts and risk levels, avoiding uniform approaches;

– **proportionality**, with interventions calibrated to the severity of the impact and the regulatory gap, and characterised by gradual escalation;
– **cross-cutting design**, through development of tools conceived to be reusable and coherent across different areas, in order to avoid duplication and fragmentation.
In this framework, co-regulation and codes of conduct are particularly relevant tools, as they can ensure flexibility and adaptation to sectoral specificities, provided they are supported by credible enforcement mechanisms and periodic review processes ensuring continuous updating of the framework in light of technological evolution.

4 Constitutional democracy and freedom of information in the age of AI

Andrea Simoncini

4.1 The constitutional dimension of freedom of knowledge, information and communication

The Italian Constitution recognises freedom of information as a fundamental and inviolable right in Article 21, where it provides that "everyone has the right to freely express their thoughts by speech, writing and any other means of dissemination" (1).

To fully understand the scope of this freedom, it must be considered from a three-dimensional perspective: the freedom to know, understood as the possibility for every individual to access information about the world, events and the opinions of others (Articles 21 and 33 of the Constitution); the freedom to inform, that is, the faculty to express one's thoughts, opinions and knowledge to the public (Article 21 of the Constitution); and the freedom to communicate, understood as the possibility of interacting and engaging in dialogue with others without interference by third parties (Article 15 of the Constitution) (2).

So understood, freedom of knowledge, information and communication is the necessary prerequisite for the realisation of many other fundamental rights: the existence of an effective space of cognitive, informational and communicative freedom is an indispensable condition for the functioning of the democratic system itself, which, being founded on the method of free competition between different political opinions, presupposes the pluralism of political supply and the existence of citizens who are truly free in their decisions because they are informed and critically aware.

Therefore, the very realisation of moral freedom (Article 13 of the Constitution) is connected to freedom of expression, without which the individual cannot fully exercise personal freedom. Likewise, Article 21 is an essential condition for education and the

development of critical thinking, as well as for scientific research itself (Articles 33 and 34 of the Constitution).

As Article 21 states, the only express limit on the exercise of this freedom is represented by public decency, which, on the basis of constitutional case law (since Judgment No. 9/1965 of the Constitutional Court), has been linked to the sphere of sexual modesty and, over time, increasingly to the protection of the development and personality of minors, abandoning the initial reference to so-called "common morality" or prevailing ethics.

Obviously, beyond this express limit, freedom of expression encounters other limits connected to constitutionally relevant interests (the right to privacy, honour and reputation, State security, etc.), further identified by the legislator — and then assessed by the constitutional judge — on the basis of a fair balance between interests of constitutional rank.

The existence of constitutional limits on freedom of expression differentiates our constitutional model from the American one, in which, as is well known, constitutional doctrine on the First Amendment and freedom of speech practically admits no effective limitations on that freedom.

One final observation — useful for understanding how our constitutional democratic system views freedom of information, especially from an evolutionary perspective — starts from the wording of the final part of the first paragraph of Article 21.

It states that "everyone has the right to freely express their thoughts by speech, writing and any other means of dissemination" (emphasis added).

By inserting the phrase "by any other means of dissemination", the framers of the Constitution proved particularly far-sighted, creating a constitutional rule projected towards the future ("future proof", as one would say today); that is, capable of including communication tools that did not yet exist at the time of drafting: from television broadcasting, to social media and, as will be seen, digital platforms.

This explains how an article written when the mass media were only newspapers and radio was able to continue inspiring and guiding legislative and judicial evolution even when television emerged and, later, during the transition from a public monopoly to an integrated public-private broadcasting system.

One need only recall, to cite some relevant examples, Judgments Nos. 225 and 226 of 1974, which established the constitutional standards to which the regulation of the public monopoly in broadcasting should be anchored; then Judgment No. 202 of 1976, which liberalised broadcasting at local level; and the warnings set out in Judgment No. 826 of 1988, followed by the adoption of Law No. 223/1990 on the regulation of the "mixed" public and private broadcasting system. Subsequent legislative initiatives followed, from the so-called third system law (Law No. 112/2004) through to the current Consolidated Law on Audiovisual Media Services (Legislative Decree No. 208/2021) (3).

Similarly, with reference to freedom of communication (Article 15), again thanks to the work of the Constitutional Court, that freedom has been extended to all available technological means, including digital channels, e-mails, chats, social platforms and, more recently, messaging services (Judgment No. 170/2023).

In conclusion, our constitutional system has proved resilient in the face of technological changes that have completely transformed the means of communication and information in recent years.

4.2 The "state" of constitutional democracy in the global context

This consideration, which can be derived from the national constitutional framework, must nevertheless be placed within the global scenario in which these transformations are taking place. And the landscape today has changed decisively compared with the "rising" phase of democracies after the Second World War: today democracy is no longer the prevailing form of political organisation in the world.

According to the Democracy Index prepared by the Economist Intelligence Unit, in 2024 only 45% of the world's population lives in regimes that can be classified as democratic, while a significant share — around 39% — is subject to authoritarian regimes and the remaining 15% lives in "hybrid" systems.

The international context is marked by growing competition between alternative models, some of which openly challenge the universality of fundamental rights and the centrality of the person: consequently, even the belief that inviolable fundamental rights must exist and be guaranteed against every form of power appears increasingly less shared and very often contested.

In this context, freedom of information assumes a crucial role: on the one hand, it is one of the fundamental indicators for measuring the "democratic quality" of a legal order; on the other, it is itself the object of tensions, restrictions and redefinitions, even within formally democratic systems.

To better understand the nature of contemporary challenges, this analysis must therefore be placed in historical perspective. Indeed, the legal protection of fundamental freedoms — what we commonly call "constitutionalism" — has never been static, but has always evolved according to the forms assumed by public and private powers capable of interfering with those freedoms.

In revolutionary constitutionalism between the eighteenth and nineteenth centuries, the power to be limited was the absolute power of the sovereign. The response was the elaboration of the principle of legality and the rule of law; law, as the expression of the general will, became the instrument through which equality and freedom were guaranteed.

However, the experience of twentieth-century totalitarianisms showed how law itself could become an instrument of oppression. Public power, instead of being bound by law, could appropriate it and use it for authoritarian purposes.

The reaction to that crisis gave rise to post-war constitutionalism, characterised by the rigidity of constitutions, the centrality of fundamental rights, the establishment of constitutional courts and, therefore, the review of the constitutionality of laws approved by the sovereign Parliament.

In that paradigm, the power to be limited was no longer only the executive power, but also the legislative power, and the Constitution established itself as the supreme norm, capable of binding all State powers.

If we continue along this historical line, we must realise that today we are witnessing the emergence of a new form of power, one that is identified neither with traditional public power nor with economic power in the classical sense.

The digital transformation of society has produced a global information infrastructure within which a plurality of essential activities take place, such as communication, information, socialisation, work and citizens' civic debate. This infrastructure is now

effectively necessary for the full unfolding of human activities and, consequently, inevitably conditions every expressive form of freedom.

Digital platforms, developed and managed by large private companies, thus exercise a power that can be defined as infrastructural, since it conditions access to a great many fundamental services, first and foremost information.

It is a new form of cybernetic power (3-bis), which influences the formation of knowledge and is therefore also relational, insofar as it structures social interactions.

This global-scale power directly affects the exercise of fundamental rights and presents strong features of opacity, posing wholly unprecedented challenges to democratic-constitutional systems as we know them.

4.3 Digital platforms as "social formations". Fundamental freedoms and private power

A theoretical issue of particular importance concerns the classification of digital platforms within constitutional law.

Article 2 of the Italian Constitution, as is well known, recognises and guarantees the inviolable rights of the person, both as an individual and within the "social formations in which his or her personality is expressed". Traditionally, such formations have been identified in contexts such as the family, local authorities, the workplace, associations, political parties and so forth.

In the current context, it is necessary to ask whether digital platforms can today be identified as new forms of social organisation, within which relations/connections that are decisive for the construction of personal identity develop.

In this regard, the dual dimension of social formations in Article 2 of the Constitution should be recalled, where it states that "the Republic recognises and guarantees the inviolable rights of the person, both as an individual and within the social formations in which his or her personality is expressed" (emphasis added).

The fact that rights must be recognised and guaranteed "within" formations expresses this duality of social formations, which are, on the one hand, a space and condition for the exercise of freedoms and, on the other, a potential source of compression and restriction of the rights of those who participate in them.

Constitutional law has historically developed predominantly within well-defined territorial boundaries, in which the State or supranational political organisations represented (and represent) the sphere within which sovereignty is exercised.

The "digital revolution" has profoundly altered this arrangement: large platforms exercise an influence that, in breadth and intensity, is comparable — if not superior — to that of States, but without being subject to the same constitutional constraints to which the latter are subject.

This character prompts reflection on the redefinition of the relationship between law and technology, on the need to adapt existing instruments of protection and the related legal categories. What emerges, above all, is the need to develop forms of international and supranational regulation, on which the other contributions in this Report dwell.

4.4 The evolution of the information and communication ecosystem

To understand more precisely how the constitutional framework within which freedom of information is exercised is changing, we must shift our attention to the transformation undergone by the so-called communication ecosystem in recent years. Until the mid-1990s, information pluralism was mainly guaranteed by the balance between the print press, radio and television; today, digital platforms, social networks, online search engines and, most recently, generative AI chatbots constitute the main "mediators" between citizens and information.

In this sense, AGCOM data show that online information has by now surpassed traditional media as the main source of news, with profound social, cultural and political implications.

According to the most recent data from the Annual Observatory on the Information System of the Italian Communications Regulatory Authority (AGCOM, 2024), one Italian in two obtains information mainly online and 50.5% of social-media users state that they receive news from digital platforms before official sources. The AGCOM

Observatory also shows that 9 Italians out of 10 own a smartphone and that as many as 87% of children between 6 and 13 own one.

Moreover, the main activity carried out by Italians on mobile devices concerns the search for information (48.8%) and communication and social networking (36%). Among minors, however, the order is reversed, with social networks dominating the information diet, bringing out new forms of socialisation and early exposure to digital content.

The AGCOM report "Media and digital literacy needs", of July 2025, also shows a widespread diffusion not only of smartphones, but also of tablets and smart TVs across all age groups, obviously with significant differences between young and older users in the use of digital content, the former being more oriented towards social media and interactive content.

This generational segmentation, however, implies the need to provide differentiated digital-education tools, capable of making citizens aware of the information flows to which they are exposed and of the functioning mechanisms of algorithms.

The pandemic experience (COVID-19) also significantly accelerated the shift to "online socialisation" and radically changed information behaviours, with many everyday activities moving into the digital world.

Platforms, therefore, are no longer "optional" tools, but indispensable infrastructures for anyone who wishes to have an ordinary social life.

In these respects as well, digital platforms — social networks, search engines and messaging applications — have assumed the role of information gatekeepers, mediating and selecting the content accessible to users.

Information power is now concentrated in the hands of large private platforms (Meta, Google, TikTok, to name only a few), and algorithms determine the content disseminated to each user, configuring a phenomenon of personalised profiling and "information filtering" for each user (the so-called filter bubble) (4).

This phenomenon entails obvious risks for pluralism, since diversity of opinions is subordinated to commercial and algorithmic logics. To this must also be added the possible risks connected to the dissemination of manipulated content (see the next section).

Moreover, with the advent of generative-AI-based chatbots (ChatGPT, November 2022) and Large Language Models (LLMs), a new and further phase has begun: users no longer simply search for content on search engines and are then directed to the relevant websites; rather, the generative AI platform, on the basis of the data on which it is trained, directly provides the answer in natural language, potentially eliminating any reference to a website to consult.

It is clear that the generation of information content through AI not only raises problems of verification and accountability, but also represents a further and formidable attack on the economic sustainability of traditional journalism.

In this regard, some recent legal actions (e.g. New York Times v. Perplexity AI, 5 December 2025) have sought concretely to challenge the conflict between intellectual property and the automatic generation of information content.

The New York Times stated in its complaint that Perplexity engaged in the "illegal copying and distribution on a massive scale" of millions of its articles to build its AI-based "answer engine". The complaint argued that "Perplexity's products directly substitute for the newspaper's content, thereby undermining its business and devaluing its journalism" and that the conduct of that AI "threatens this legacy and prevents the free press from continuing to perform its role in supporting an informed citizenry and a healthy democracy."

Today, therefore, the digital information space is no longer composed of an infinity of websites simply intermediated by platforms — search engines or social media — but is very rapidly contracting and concentrating around chatbots and LLMs that respond directly to information needs, causing the websites of origin to disappear.

4.5 Disinformation as a constitutional problem and the Romania case as a "constitutional laboratory"

As mentioned above (see previous section), one of the problems connected to the dissemination of information through AI tools and chatbots concerns the verification and reliability of the information disseminated.

Disinformation, in its contemporary configuration, can no longer be interpreted as a marginal or pathological phenomenon of the information ecosystem; it constitutes a structural element of the functioning of digital platforms and consequently becomes a problem of constitutional nature.

Freedom of information requires the presence of a plurality of sources, full accessibility of information and the critical capacity of recipients.

In the digital context, these conditions are often profoundly altered. The concentration of information sources, the personalisation of content and the information asymmetry between platforms and users compromise the very functioning of democracy.

Moreover, according to a study by the EUI Observatory on Information and Democracy (5), of December 2024, digital platforms, unlike traditional media, can derive significant profit from disinformation.

Indeed, in 2021, websites publishing disinformation generated as much as USD 2.6 billion in advertising revenue globally, with Meta earning at least USD 30.3 million.

The monetisation of disinformation raises existential issues for freedom of information, since it transforms a fundamental right into a good traded for profit, with systemic effects on the formation of public opinion and the quality of democracy. A genuine market for disinformation is thus created, in which truth loses economic value.

In this context, an important decision adopted by the Romanian Constitutional Court in December 2024 constitutes one of the most significant examples of conflict between digital technologies, freedom of information and electoral processes in the European constitutional context (6). The constitutional judges in Bucharest annulled the entire procedure for the election of the President of the Republic that had begun on 24 November 2024, ordering the Government to set a new date for the elections, because of serious irregularities “throughout the entire duration and in all phases” of the vote, attributable to the non-transparent use of digital technologies, the use of artificial intelligence in the electoral campaign and undeclared electoral financing by one of the candidates.

On the basis of information notes made public by the Government, referred to in the reasoning but without analytically reporting the facts described, the Court held “that the electoral process for the election of the President of Romania was vitiated

throughout its duration and in all its phases by multiple irregularities and violations of electoral legislation that distorted the free and fair nature of the vote cast by citizens and the equal opportunities of electoral competitors, affected the transparent and fair nature of the electoral campaign and failed to comply with the legal rules on its financing. All this had the convergent effect of failing to comply with the essential principles of democratic elections (…) through the non-transparent use, in violation of electoral laws, of digital technologies and artificial intelligence in the conduct of the electoral campaign, as well as through the financing of the electoral campaign from undeclared sources, including online."

The Romanian Court acted on the basis of its "general" function as guarantor of the Constitution and thus decided to interpret very extensively its "special" competence as electoral judge.

Beyond doubts at the procedural and competence level, the decision is relevant because it starts from the finding that the exercise of constitutional freedoms today takes place in "digital space", so much so that the violations complained of were all perpetrated by means of new cybernetic technologies. Electoral campaigns, in particular, take place (predominantly) through new digital media, with respect to which the means of legal protection must be completely recalibrated.

With reference to this case, beyond the shadows surrounding the Romanian Court's intervention, this action shows how, in the era of fake news, it is increasingly decisive to provide for transparent forms of independent control of electoral processes — particularly in direct elections — and that such control must, where possible, be preventive, since ex post judgments could fuel very strong tensions internally.

The Romanian Court decided to assign itself review of the electoral procedure, at least "integrating" the existing legislation and exercising a power which, precisely because it is unregulated, risks setting off a series of political chain reactions that would be difficult to contain.

It should nevertheless be noted that fundamental support for the initiative of the Bucharest judges came from the European Commission itself, which, the day before the decision — on 5 December 2024 — issued against the digital platform TikTok (considered by the Romanian Government to be primarily responsible for the

disinformation) an order to preserve data relating to ongoing electoral processes, between 24 November 2024 and 31 March 2025.

In fact, through that action the Commission strongly corroborated the hypothesis of interference in the Romanian elections by the Chinese platform (allegedly manipulated by Russian principals).

The significance of this decision, beyond its media coverage, lies in the fact that at European level what can now be defined as a genuine "digital acquis" (7) is increasingly consolidating: in effect, a regulatory corpus unique in the world concerning the impact of digital transformation on information tools, through to the regulation of political communication (8).

4.6 Conclusions: towards a European digital constitutionalism

Freedom of information, viewed diachronically, is today at the centre of a tension that affects the entire edifice of contemporary constitutionalism.

It is not simply a matter of adapting existing categories to new technologies, but of addressing a genuine genetic mutation in the relationship between power, knowledge and democracy.

The first element that clearly emerges is that freedom of information can no longer be guaranteed only as the absence of interference by public power. That conception, adequate in the context of liberal and post-war constitutionalism, is insufficient in the face of private platforms of global scale. In this context, the threat to fundamental freedoms no longer derives only from risks linked to censorship or repression, but also from those linked to the manipulation, selection and orientation of information flows.

Secondly, analysis of the digital ecosystem shows how information power has progressively become concentrated in the hands of a few global actors. Digital platforms and artificial-intelligence systems do not merely facilitate access to information; they determine its structure. This phenomenon raises a crucial question: whether such entities should be classified as mere intermediaries or instead considered holders of responsibilities analogous — though not identical — to those traditionally attributed to publishers.

The difficulty of answering this question reflects a deeper tension between two opposing needs: on the one hand, protection of freedom of expression and

technological innovation; on the other, the need to guarantee the quality and reliability of information. In this unstable balance, the risk is that stricter regulation could restrict freedom, while insufficient regulation could undermine the very conditions of democracy.

A third profile concerns disinformation, which emerges as one of the main factors destabilising democratic systems. As seen, it is not a marginal phenomenon and, indeed, its propagation affects the ability of citizens to form autonomous, free and informed opinions.

In this sense, the 2024 decision of the Romanian Constitutional Court represents a paradigmatic signal: for the first time, digital disinformation is considered capable of compromising the validity of an electoral process. Beyond the undoubted criticalities of the ruling, it highlights a crucial acknowledgement: democracy cannot be reduced to a formal procedure, but requires substantive conditions relating to correct information for those exercising fundamental rights.

A final element of reflection concerns the growing role of European law, which will be examined in detail later.

The Union's regulatory interventions — from the Digital Services Act to the Artificial Intelligence Regulation — outline a model of regulation that seeks to combine innovation and protection of fundamental rights. These instruments do not merely regulate technical aspects, but introduce principles of constitutional nature, such as transparency, accountability and the management of systemic risks.

In fact, they find themselves performing a genuine constitutional substitute function in the face of the unprecedented and extremely rapid phenomena that we have tried to outline.

It is therefore possible to speak, with ever greater awareness, of an emerging European digital constitutionalism, understood as a set of rules and principles aimed at governing technological power in a rights-protective key. However, this process is still in consolidation and presents numerous criticalities; above all, the risk of excessive fragmentation and overproduction of rules, which creates very significant difficulties in the effective application of those rules (the recent proposal for the Digital Omnibus Package is a sign of this awareness).

The possibility of accessing unlimited information, the personalisation of content and continuous interaction with automated systems also require active media and digital literacy policies, as highlighted by the AGCOM reports discussed above.

With regard also to the protection of vulnerable persons, particularly minors, the risks linked to the pervasiveness of content and the difficulty of control assume particular relevance. The protection of minors is, indeed, the first testing ground of the emerging European digital constitutionalism.

Looking ahead, the main challenge consists in rethinking the form of constitutional democracy in light of the new forms of digital power. This implies, on the one hand, the development of new legal categories and, on the other, the strengthening of existing instruments.

In particular, greater algorithmic transparency, greater platform accountability, better development of digital-education tools and stronger international cooperation — necessary to address global phenomena — must be required.

Ultimately, freedom of information requires an integrated approach capable of holding together the legal, technological and economic dimensions. Otherwise, the risk is the progressive erosion of the authenticity of democracy itself in the age of artificial intelligence, in which formally free citizens risk being heavily conditioned in the formation of their opinions by the technological systems they use.

Notes

(1) A. Pace - E. Manetti, Art. 21. Rapporti civili. La libertà di manifestazione del pensiero, in Commentario della Costituzione, founded by G. Branca and continued by A. Pizzorusso, Bologna-Rome, 2006;

(2) P. Barile - E. Cheli, entry Corrispondenza (libertà di), in Enc. Dir., vol. X, Milan, Giuffrè, 1962, pp. 743 ff.;

(3) P. Caretti – A. Cardone, Il diritto dell'informazione e della comunicazione nell'era dell'intelligenza artificiale. Seconda edizione, Milan, Il Mulino, 2024, pp. 120 ff.;

(3-bis) A. Simoncini, Potere cibernetico e futuro del diritto costituzionale, in Quaderni costituzionali, No. 1/2026

(4) E. Longo, Dai big data alle «bolle filtro»: nuovi rischi per i sistemi democratici, in Percorsi Costituzionali, 12/2019, pp. 29 ff.;

(5) Observatory on Information and Democracy EUI, Information Ecosystems and Troubled Democracy, A Global Synthesis of the State of Knowledge on News Media, AI and Data Governance, in www.observatory.informationdemocracy.org, 3 December 2024;

(6) Constitutional Court, Judgment No. 32 of 6 December 2024; for an initial analysis of the decision, see A. Simoncini, L'annullamento delle elezioni presidenziali in Romania. Luci ed ombre di una divisiva decisione costituzionale, in Quaderni costituzionali, 1/2025, pp. 234 ff.;

(7) A. Bogucki – A. Engler – C. Perarnaud and A. Renda, The AI Act and emerging EU digital acquis. Overlaps, gaps and inconsistencies, in www.ceps.eu, 14 September 2022.

(8) On the one hand, one may think of the Regulation on transparency and targeting in political advertising (2024/900/EC) and the interpretative declaration of the Venice Commission; on the other, of the aforementioned intervention by the European Commission against TikTok, through the powers assigned to it by the Digital Services Act (2022/2065/EC), which — as noted — externally legitimised the action of the Romanian Court.

5 Generative AI, disinformation and hate speech: systemic risks and regulatory levers for AGCOM

Giovanni Boccia Artieri

5.1 Introduction: AI as a discursive environment and cognitive infrastructure

Artificial intelligence (AI) cannot be regarded as a mere set of external technical tools; it must be understood as a pervasive informational environment that intervenes in the very conditions of thought. It acts as a cognitive infrastructure and symbolic environment capable of reshaping everyday practices, the grammars of attention and forms of social imagination. Generative AI marks a decisive shift because it automates and scales significant portions of cognitive work through the production of texts, images and simulations, directly redefining what appears credible, authoritative and relevant.

These systems tend to operate as epistemic devices: they structure the conditions in which thought takes shape, is recognised and is validated. Through statistical modelling, they transform vast data archives into probabilistic surfaces of meaning, offering normalised versions of knowledge that may conceal the biases and gaps of the archives from which they learn. By aligning themselves with the statistical regularities of past discourse, they can act as an "epistemic mask", marginalising dissonant voices and situated or counter-hegemonic knowledge.

Systemic risks therefore emerge for the integrity of the communication ecosystem. Information manipulation takes the form of synthetic content such as deepfakes and voice cloning, while discursive degradation is fuelled by hate speech and online toxicity. These phenomena are linked to algorithmic amplification, attention economies and micro-targeting. The habit of receiving immediate, well-formed answers favours a relationship with knowledge centred on the "solution" rather than on verification and problematisation.

For the Italian Communications Regulatory Authority, AI is a cross-cutting factor affecting fundamental rights and protection mechanisms. This contribution places these issues at the intersection of the Digital Services Act (DSA) and the AI Act. As Digital Services Coordinator, AGCOM is called upon to supervise these risks not merely through technical oversight, but through situated human judgment. The chapter provides an operational compass for regulatory action through ex ante measures, in itinere tools and ex post interventions.

5.2 Critical dimensions: information manipulation and discursive degradation

The massive integration of generative AI into communication processes has amplified pre-existing systemic threats and produced a qualitative leap in the creation and dissemination of problematic content. These systems do not merely transmit information: they act as epistemic devices that restructure the criteria of truth and reliability.

5.2.1 Information manipulation and the era of synthetic content

Contemporary information manipulation relies on advanced synthetic content — deepfakes, face swapping, lip-syncing and voice cloning — which destabilises authenticity and makes it harder to distinguish events from artificial reconstructions. Automated high-quality generation turns falsification from an artisanal exception into an industrialisable, replicable and adaptable process.

Generative AI can produce highly plausible false content at almost zero marginal cost. This lowers technical barriers and enables continuous production of many variants calibrated to different publics. The result is not only more deceptive content, but a qualitative transformation of information disorder: synthetic images, audio and texts become socially plausible artefacts that manipulate not only what circulates, but what appears probable and therefore credible.

Another intrinsic risk is hallucination: inaccurate or invented information presented with an authoritative tone. Scientific literature shows that hallucinations are structural effects of generative models, which optimise coherent sequences rather than

adherence to verifiable truth. In a context where online sources dominate information consumption, the ability of these systems to "write like us" and "speak like us" makes distinguishing reliability from unreliability a permanent cognitive task.

The era of synthetic content introduces two vulnerabilities. The first is deceptive: convincing audiovisual evidence can be fabricated and circulated at the speed of attention. The second is epistemic: uncertainty erodes trust and normalises the idea that "we no longer know what is true". Deepfakes therefore matter not only for direct persuasion, but also for the production of doubt and the so-called liar's dividend, whereby authentic content can be dismissed as artificial.

Voice cloning further lowers the threshold of manipulation because the voice is perceived as intimate and immediate, a marker of identity and presence. Synthetic audio is highly effective in disinformation and fraud, while its detection remains technically contested and vulnerable to adversarial strategies. Detection and generation co-evolve, making information security a race between synthesis and verification.

Manipulation in the synthetic era also concerns the infrastructure of trust. The most promising response combines detection with provenance: asking not only whether something is false, but where it comes from and what transformations it has undergone. Standards such as C2PA aim to provide verifiable metadata on origin and modification, shifting attention from hunting falsehoods to building chains of authenticity, while recognising their practical limits.

Overall, the synthetic era does not simply produce more disinformation; it reconfigures the conditions of public credibility. It makes falsification scalable and doubt scalable. The public sphere risks sliding into post-reliability, where plausibility replaces proof and attention is captured by communicative objects optimised to appear true regardless of their actual status.

5.2.2 Discursive degradation: hate speech and automated toxicity

The second critical dimension is discursive degradation, fuelled by hate speech, incivility and forms of e-bile: online practices marked by resentment, invective, contempt and verbal aggression. Online hatred is not mere background noise but a grammar of interaction that combines denigration, threat and humiliation, often

targeting exposed subjects and groups. Platform affordances such as relative anonymity, asynchronicity and lack of face-to-face contact lower the social cost of aggression.

Digital tools also facilitate swarming, in which users coalesce around events or persons, reinforcing discriminatory practices through distributed and repeated attacks. Hate often takes the form of a harassment assemblage: comments, memes, doxxing, hostile quotations and other micro-acts that together produce pressure and silencing. Incivility can polarise perceptions and reduce the quality of political debate.

In this context, generative AI directly affects opinion formation through hyperpersuasion based on adaptive alignment and empathic optimisation. Models align with user preferences, confirm expectations and reinforce biases through successive micro-adjustments. Recent research suggests that personalised conversational systems can be more persuasive than human debate when they have even limited information about the interlocutor.

This effectiveness is not generic: argumentation is shaped around demographic and psychological traits, producing hyper-personalisation that exploits cognitive asymmetries and reduces exposure to dissonant views. It can reinforce echo chambers, simulate false consensus and weaken public disagreement as a democratic practice, replacing deliberation with cognitive delegation to machine-generated outputs.

A further risk is automated toxicity: the large-scale production of hostile language. With bots and generative models, comments, insults, insinuations and dog whistles can be industrialised, varied to avoid filters and adapted to local contexts. Computational propaganda turns visibility into credibility, making orchestration appear spontaneous. LLMs used for moderation create an additional tension. They may help detect hostile language, but research points to opacity and limits in understanding implicit references, irony or community context. This can produce false positives on emancipatory speech and false negatives on coded hate. Automation therefore affects both the production and the institutional management of hate.

The ecosystem is sustained by business models that monetise attention and treat toxic messages as a negative externality of advertising. Swarming and computational propaganda can transform marginal voices into perceived political relevance.

Discursive degradation in the AI era is therefore a reconfiguration of the conditions of public discourse: toxicity becomes scalable and adaptive, while persuasion becomes personalised and less observable.

5.2.3 The "black box" effect and the challenge of accountability

The risks described are aggravated by the opacity of many contemporary deep-learning models. AI often operates as a black box not because nothing is known, but because the chain linking data, training, architecture and outputs is difficult to reconstruct in a comprehensible and verifiable way, especially in complex, multi-component and continuously updated systems.

Public accountability cannot be reduced to an ex post explanation of a single output. There is no single definition of interpretability or a single way to measure it. The need for explanation varies according to domain, risk and addressee. In high-stakes contexts, the solution is not only to explain better, but to design more controllable, documented and, where possible, intrinsically interpretable systems.

The black-box effect becomes a political and regulatory problem because opacity shifts the possibility of understanding and contesting decisions away from public spaces and affected subjects. What is needed is verifiable evidence on data, metrics, objectives and constraints. Tools such as model cards and datasheets for datasets do not fully open the black box, but create a minimum basis for traceability, comparison and informed contestation.

AI incidents, including automated disinformation and information harms, are thus a crucial regulatory issue. As Digital Services Coordinator for Italy, AGCOM must supervise risks affecting fundamental rights and democratic integrity. Harm often emerges from design choices — recommendation, ranking, frictions, moderation, advertising and engagement patterns — rather than from a single piece of content. The challenge is to move from ex post supervision to structural oversight of algorithmic architectures, from single falsehoods to process traceability, and from declaratory transparency to independently verifiable control.

5.3 Mechanisms of algorithmic amplification and the attention economy

These systemic risks draw their effectiveness from a technological and economic architecture linking automated production, micro-targeting and algorithmic attention management. AI multiplies scale and precision, turning information disorder into an industrial process. Platforms govern visibility and relevance through opaque ranking and recommendation systems, while the attention economy rewards emotionally charged, polarising or toxic content.

5.3.1 Scalable production and psychographic micro-targeting

Generative AI automates cognitive work and makes manipulative content replicable at minimal cost. It combines with micro-targeting by shaping messages around the vulnerabilities or demographic traits of specific interlocutors. Research indicates that personalised LLM-based argumentation may be especially persuasive in online debate. Psychographic micro-targeting research shows that messages aligned with personality traits can affect attitudes and voting intentions. Personalisation operates not only through interests and demographics, but through compatibility between communicative frames and individual predispositions. This produces hyper-personalised persuasion that can exploit cognitive asymmetries.

Micro-targeting is therefore both a distribution technique and a technology for adapting messages. Persuasion becomes less observable and harder to scrutinise because it is fragmented into many individualised variants, potentially eroding the common and verifiable dimension of political discourse.

5.3.2 Recommendation systems and algorithmic feedback loops

Recommendation systems determine the visibility and circulation of content. They act as cognitive filters, restructuring information experience into assisted sequences of exposure and selection. Through positive feedback loops, each user interaction feeds learning mechanisms, increasing the platform's ability to retain attention and reinforcing the economic value of the infrastructure.

This process can generate epistemic exclusion. Algorithmic personalisation may reduce incidental exposure to dissonant content and normalise partial versions of knowledge. Monitoring is difficult because architectures are opaque and systemic harm often derives not from individual illegal content, but from the combination of ranking, engagement patterns and design choices that determine visibility and speed.

5.3.3 Algorithmic awareness and asymmetries of protection

AGCOM data reveal significant asymmetries in awareness of these mechanisms. More than half of Italians aged 14 and over state that they know about recommendation algorithms, but the share is much lower among older people; only around half are aware of tools for personalising their experience. This algorithmic-literacy gap reduces users' ability to attribute causality to algorithms and exercise informational agency.

Protection asymmetries increase because attention-based business models monetise engagement. Toxic or polarising content may be tolerated where it sustains time spent on platforms. Users' most common reaction is often avoidance of the channel or platform rather than proactive use of reporting, source-verification or preference-management tools.

Regulatory intervention must therefore move beyond reaction to single episodes and focus on structural supervision of architectures. The DSA imposes obligations for systemic-risk management, including risk assessments and independent audits for very large platforms. The aim is to restore visibility, verifiability and public control at the level where social reality is increasingly produced: algorithmic infrastructures of distribution.

5.4 The regulatory framework: intersections between the AI Act and the Digital Services Act

The European regulatory landscape is shifting from reaction to single illegal content towards systemic and architectural supervision of how platforms produce visibility, amplification and protection asymmetries. The DSA targets design choices — recommender systems, advertising, moderation, terms of use and data practices — while the AI Act operates upstream on design, market placement and use of AI systems,

including transparency obligations for synthetic content and human-machine interaction.

The formula "AI Act upstream, DSA downstream" is useful but simplified. In practice, the two frameworks intersect along the chain of responsibility between model developers, deployers and platforms. A formally compliant generative model can create systemic harms when embedded in recommendation, targeting and moderation systems, while a platform may comply formally with DSA content obligations and remain opaque about the design choices and technological dependencies that generate risks.

The intersection between the two regulations may create grey areas of attribution and distributed responsibility. Each actor can claim compliance within its own perimeter while the overall effect remains difficult to govern. The EU addresses this through process obligations — risk assessment, audit, reporting — and transparency obligations such as disclosure and labelling. The risk is that accountability becomes largely documentary unless accompanied by genuine verifiability and intervention on operational logics.

A concrete sign of this architectural shift is the annual DSA risk-landscape cycle: the Commission and the Board of Digital Services Coordinators publish recurring reports on prominent systemic risks and mitigation measures. This moves supervision from episodic cases towards comparative and cumulative oversight. Yet process and transparency obligations can become low-density compliance unless backed by access to data, independent verification and shared methodological standards.

- The first condition is access to the data and information needed to verify platform claims. Without access, risk assessments remain self-descriptive and reflect the cognitive perimeter of the platform rather than an independent analysis of risk.
- The second condition concerns the quality and independence of verification. If an audit cannot measure the effectiveness of mitigations through robust indicators, it risks becoming a ritual procedure, formally correct but substantively weak.

- The third condition is the construction of shared methodological and metric standards that make assessments comparable over time and across platforms, reducing arbitrariness in definitions of risk and success criteria.

Critical analyses of the first rounds of risk assessment show this structural tension: without stable data access and common criteria, governance risks becoming "accountability by report", rich in formal documentation but weak in its ability to affect design choices and incentives that feed amplification.

5.4.1 AGCOM as Digital Services Coordinator and the management of systemic risks

As Digital Services Coordinator, AGCOM is the national pivot of DSA implementation, linking the European level of the Commission with cooperation among coordinators and developing procedures, tools and enforcement capacity. Its role is not limited to removal or sanctions on individual content; it is to make operational the DSA logic of systemic-risk regulation.

This approach shifts attention from "what circulates" to "how it circulates". For AGCOM this means assessing whether large platforms, especially VLOPs, can identify and mitigate risks affecting information pluralism, the integrity of public debate and fundamental rights. The key issue is the combination of amplification mechanisms, engagement design and micro-targeting that can turn marginal signals into perceived consensus.

The Coordinator's action depends on verifiable evidence about platform practices. AGCOM's role is to build conditions of contestability: access to data and documentation, ability to evaluate risk assessments and mitigations, independent verification and shared methodological standards. Compliance must translate into changes in design practices.

AGCOM also operates within a multi-level network of European and international cooperation. Because systemic risks are scalable, replicable and cross-border, their management requires coordination across enforcement, pluralism protection and rapid response, moving from sporadic cases to stable supervision of algorithmic infrastructures.

5.4.2 Transparency obligations and algorithmic accountability

The integration between AI Act transparency obligations and DSA systemic-risk mitigation is a central regulatory lever. In a context of widespread syntheticity, transparency is not merely moral or communicative: it helps reduce both the proliferation of synthetic content and the strategic doubt that feeds the liar's dividend. The AI Act requires that generated or manipulated content be recognisable as artificial, especially in cases of deepfakes and plausible simulations.

This moves part of protection upstream, reducing information asymmetry between producers and users and enabling faster identification of synthetic content in high-exposure contexts such as elections, crises, conflicts and news events. Labelling must, however, be supported by technical infrastructure enabling tracking in rapid, multilayered circulation environments.

a) Watermarking and content-integrated markings are relevant, while raising known problems of robustness and persistence across sharing chains.
b) Provenance standards attach verifiable metadata that reconstruct the origin and transformation of content. C2PA is an advanced reference for chains of authenticity based on signed and verifiable metadata, especially for institutional and journalistic contexts.

Marking, labelling and provenance become genuine levers of risk governance only if they are actionable within visibility architectures. The key is not only whether content is labelled, but what the label produces: frictions, contextual warnings, verification priority, de-amplification, targeting limits or moderation escalation.

The second axis concerns accountability for models and systems that incorporate them. Black-box effects make it difficult to reconstruct fully the chain from training to output, especially in updated and multi-component systems. Accountability must therefore become documentary responsibility: evidence on purposes, limits, performance, risks and acceptable or problematic uses, through instruments such as model cards and datasheets for datasets.

Operationally, the goal is not to accumulate documentation but to transform transparency into contestability. The Authority should verify what marking and disclosure mechanisms are implemented, whether they persist through download, re-

upload and compression, whether they affect ranking and recommenders, and whether interoperable provenance standards are adopted. For model accountability, documentation must also be available where third-party models are integrated as services, with metrics for public-risk cases and edge cases such as satire, parody, journalism and public interest.

5.4.3 Protection of vulnerable users and minors

A priority focus is the protection of minors and vulnerable users from manipulative or inappropriate content and from engagement architectures that produce cumulative harm. The issue is not only removing harmful content, but supervising the technical conditions that make it reachable, persistent and repeatable: recommendation chains, profiling, absent frictions and reward dynamics. This is the meaning of Article 28 DSA, requiring platforms accessible to minors to ensure high levels of privacy, safety and protection.

Within this framework lies the still-developing issue of cognitive debt: the hypothesis that intensive and unmediated use of generative assistants may encourage cognitive offloading and reduce engagement in learning tasks. Preliminary experimental evidence suggests that AI assistance can shift writing from internal elaboration towards selection and validation of machine outputs, producing more similar texts and recurrent structures. These findings should be treated as risk signals, especially for minors.

A further cumulative effect concerns linguistic standardisation. If generative models become mass media for writing, rewriting and conversation, their outputs may stabilise certain forms of expression. Millions of users relying on the same tools may absorb and reintroduce model-suggested styles and structures, creating a feedback loop between AI outputs and human communication.

The possible consequences concern linguistic variety and expressive registers. Highly compatible “average” solutions may reduce idiolects, local registers and creative deviations, while model-preferred tones tend to be neutral, balanced and predictable. The risk is not total uniformity, but statistical pressure towards dominant expressive forms that are easier and more frequently reused.

It is important to avoid the rhetoric of minors as automatically competent "digital natives". Skills vary systematically even among young users and are linked to cultural capital and social conditions. Algorithmic opacity and adaptive persuasion affect most strongly those who lack tools to recognise them.

For minors, risks are also linked to rabbit holes: recommendation paths that, from minimal signs of interest or vulnerability, can increase exposure to harmful content such as eating disorders, self-harm, violence, pornography or extremism. Literature and policy reports show the need for measures that affect design, not only downstream moderation.

Recent interventions on dangerous social challenges show that rapid reduction of exposure is possible in emergencies. The challenge is to make this capacity structural, through verifiable obligations on design and distribution, because harm arises above all from repetition and amplification.

Another vulnerability is hyperpersuasion: conversational systems can adapt tone and argumentation to user traits. For minors, the critical issue is not only political opinion, but habituation to fluent and reassuring answers as a substitute for competence, normalising a relationship in which the machine becomes an authoritative interlocutor without educational friction.

A prevention strategy must integrate literacy, educational mediation and institutional supervision. Preventing cognitive debt in minors requires multiple levers acting on skills, everyday practices and the environmental conditions of use.

1. Prompt culture as reflective practice. Prompting should be taught not as a technique of efficiency, but as clarification of thought: making the problem explicit, defining context and quality criteria, and maintaining the distinction between linguistic fluency and content reliability.
2. Algorithmic literacy and active curation. Filters must be made intelligible: how recommenders and rankings shape perception and can trigger rabbit holes. This awareness should be combined with practical use of personalisation and reporting tools, shifting from passive consumption to conscious feed management.

3. Enabling parental mediation. Restriction alone is often insufficient; comparative evidence points to accompaniment and co-use strategies that turn interaction into an opportunity for critical skills development.
4. Alliance between schools and institutions. Vertical curricula in digital citizenship and algorithmic literacy are needed as stable public infrastructure, together with institutional supervision of the effectiveness of DSA measures for minors.

In short, protecting minors and vulnerable users means avoiding the total delegation of interpretative work to machines, preserving situated judgment and the ability to problematise responses within environments designed to reduce exposure, repetition and persuasive vulnerability.

5.5 Operational proposal: levers of intervention for AGCOM

This section translates the analysis into an operational compass for the Authority as Digital Services Coordinator. The goal is not to chase individual episodes, but to make measurable and contestable the architectures that produce risk: recommendation, ranking, advertising, moderation and engagement design. AI Act and DSA should be treated as a single governance device.

5.5.1 Ex ante measures: building the infrastructure of trust

Preventive measures reduce information asymmetry between platforms, users and authorities and prevent widespread syntheticity from becoming an automatic multiplier of disorder and distrust.

a) Actionable algorithmic transparency (not declaratory). Define minimum verifiable requirements for making ranking and recommendation criteria intelligible: optimised objectives, input signals, frictions, de-amplification policies and escalation conditions. Transparency must be a condition of contestability.

b) Documentary responsibility for models and data. Require and standardise model cards and datasheets, focusing on limits, known biases, adverse-condition

performance, edge cases and updating procedures. The purpose is to build comparable evidence for audit and independent control.

c) Labelling and provenance of synthetic content as infrastructure, not a sticker. Promote robust marking and labelling for deepfakes and synthetic content, and interoperable provenance standards such as C2PA. Labels should activate frictions, verification priorities, targeting limits or de-amplification.

d) AI literacy as critical mindset and prevention of cognitive delegation. Support literacy programmes that teach the distinction between fluency and reliability, source verification, recognition of persuasive patterns, understanding of algorithmic filters and active curation practices.

To avoid declaratory transparency, minimum evidence must be defined: standard reporting on optimised objectives, signals, frictions, de-amplification policies and escalation criteria. For labelling and provenance, effectiveness must be measured along the chain: label retention after download, re-upload and compression, and observable distribution effects such as frictions, targeting limits and de-amplification.

5.5.2 In itinere tools: supervision, data and systemic cooperation

Continuous supervision measures whether mitigations work over time and identifies rapid changes such as new synthetic formats, amplification tactics and audience shifts.
a) Monitoring systemic risks and auditing visibility architectures. Strengthen analysis of recommender and ranking systems by measuring exposure, reach and propagation speed for risk classes such as synthetic disinformation, toxicity and rabbit holes affecting minors.
b) Data access and independent research (DSA Article 40). Make data access operational for qualified researchers and independent laboratories through clear privacy-by-design protocols, minimisation and secure environments. Without access, risk assessments remain self-descriptive; with access, they become verifiable.

c) Inter-authority cooperation and European coordination. Build a stable circuit with privacy, competition and consumer-protection authorities and the European DSC network, because risks are cross-border and multi-regime.

Audits must focus on outcomes, not merely processes. Key metrics include exposure, reach, velocity, reiteration and, where relevant, rabbit-hole depth. Mitigations should be assessed on measurable before/after variations in these indicators.

5.5.3 Ex post actions: accountability, remedies and response protocols

Downstream measures must prevent violations from becoming merely a cost of doing business and must generate regulatory learning.

a) Design-based enforcement. In cases of systemic violations, corrective and sanctioning measures should affect processes and design: frictions, targeting limits, de-amplification, recommender changes and enhanced reporting. The aim is to change the conditions that produce risk, not merely remove individual content.

b) Incident-response protocol and AI-incident observatory. Establish monitoring and classification of incidents — viral synthetic disinformation, labelling errors, hallucinations in sensitive contexts and automated toxic escalations — with rapid-response procedures and channels for correction and counterbalancing. The incident archive should feed periodic updating of ex ante guidelines.

For incident response, effectiveness should be measured by response times (detection–mitigation–communication) and documented reduction of reach and propagation, including lowering diffusion curves, reducing speed and containing reiteration. Incidents should feed a cycle of adaptive governance.

Phase	Lever	What it requires in practice	Expected evidence/output

Ex ante (prevention)	Actionable transparency	Minimum verifiable requirements on optimised objectives, signals/features, frictions, de-amplification policies and escalation criteria	Standard transparency scheme and comparable reporting
	Mandatory documentation	Model cards/datasheets on limits, biases, adverse-condition performance and edge cases (minors, public interest)	Verifiable documentation for audit and contestation
	Synthetic content	Labelling/marking and disclosure under the AI Act with robustness to re-upload/compression and integration into distribution logic	Persistent labels and activation of frictions, limitations and de-amplification
	Interoperable provenance (C2PA)	Adoption of provenance standards and verifiable metadata along the chain	Consultable and verifiable chain of authenticity
	AI literacy	Distinction between fluency and reliability; verification practices; awareness of filters; active curation	Programmes and materials for critical skills and reduced cognitive delegation

In itinere (continuous supervision)	Outcome-oriented audits	Measure exposure/reach/velocity, rabbit-hole depth, reiteration and impact of mitigations	KPIs and effectiveness reports on mitigations, not only compliance
	Data access (DSA Article 40)	National protocol for independent research access, privacy-by-design and secure environments	Traceable data access and reproducible studies/external checks
	Multi-authority coordination + DSC network	Common standards, information exchange and harmonised enforcement	Shared guidance and coordinated actions on cross-border risks
Ex post (remedies)	Design-based enforcement	Remedies on frictions, targeting limits, de-amplification and recommender changes, not only removal	Binding corrective measures affecting the distribution architecture
	AI-incident observatory + rapid response	Incident taxonomy, response protocols and cyclical updating of guidelines	Operational incident response and regulatory learning

Table 1 Operational matrix of intervention levers: ex ante / in itinere / ex post

5.6 Conclusions: infrastructure of trust and adaptive governance

Generative AI does not merely add new content to the information flow; it reconfigures the conditions of production, circulation and credibility of public discourse, linking automated writing and audiovisual production, micro-targeting and recommendation architectures that turn attention into value. Democratic vulnerability lies not only in more falsehoods, toxicity or incivility, but in the way these phenomena become scalable, persistent and adaptive, affecting pluralism, authenticity attribution, the legitimacy of dissent and the protection of vulnerable users.

The regulatory response cannot be limited to ex post removal or declaratory transparency. It must aim at the contestability of architectures. The intersection between AI Act and DSA provides complementary tools: marking and labelling obligations, provenance for synthetic content, systemic-risk assessments and mitigations, audits and data access, and remedies affecting ranking, recommendation, targeting and frictions. The operational compass proposed here aims to consolidate adaptive governance: ex ante measures building an infrastructure of trust, in itinere supervision making risks and mitigations verifiable, and ex post actions transforming incidents into institutional learning. The goal is not a sterilised public sphere, but a digital environment where freedom of expression and pluralism coexist with protection of minors and vulnerable users and with the integrity of democratic debate.

Bibliography

AGCOM (2025). Artificial Intelligence. 2025 Report (internal document / working draft). Rome: Italian Communications Regulatory Authority.

Amnesty International (2023). Dragged into the Rabbit Hole: New Evidence of TikTok's Risks to Children's Mental Health (report). London: Amnesty International. https://www.amnestyusa.org/reports/dragged-into-the-rabbit-hole-new-evidence-of-tiktoks-risks-to-childrens-mental-health/

Bender, E. M., Gebru, T., McMillan-Major, A., & Shmitchell, S. (2021). On the dangers of stochastic parrots: Can language models be too big? In Proceedings of the 2021 ACM

Conference on Fairness, Accountability, and Transparency (FAccT '21) (pp. 610–623). ACM.

Bennett, W. L., & Livingston, S. (2018). The disinformation order: Disruptive communication and the decline of democratic institutions. European journal of communication, 33(2), 122-139.

Boccia Artieri, G. (2025). Sfiduciati. Democrazia e disordine comunicativo nella società esposta. Milano: Feltrinelli.

C2PA (Coalition for Content Provenance and Authenticity) (2025). C2PA Specifications Overview: Latest Version 2.2 (released May 2025). https://c2pa.wiki/specifications/

Castaño-Pulgarín, S. A., Suárez-Betancur, N., Vega, L. M. T., & López, H. M. H. (2021). Internet, social media and online hate speech: Systematic review. Aggression and Violent Behavior, 58, 101608.

Chaney, A. J. B., Stewart, B. M., & Engelhardt, B. E. (2018). How algorithmic confounding in recommendation systems increases homogeneity and decreases utility. In Proceedings of the 12th ACM Conference on Recommender Systems (RecSys '18) (pp. 224–232). ACM.

Chesney, R., & Citron, D. K. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. California Law Review, 107, 1753–1819.

European Commission (2025). Digital Services Act report lays out landscape of systemic risks online. Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/news/digital-services-act-report-lays-out-landscape-systemic-risks-online

Crawford, K. (2021). The Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence. New Haven, CT: Yale University Press.

Eslami, M., Rickman, A., Vaccaro, K., Aleyasen, A., Vuong, A., Karahalios, K., Hamilton, K., & Sandvig, C. (2015). "I always assumed that I wasn't really that close to [her]": Reasoning about invisible algorithms in news feeds. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15) (pp. 153–162). ACM.

European Board for Digital Services (2025). First report of the European Board for Digital Services in cooperation with the Commission pursuant to Article 35(2) DSA on

the most prominent and recurrent systemic risks as well as mitigation measures (18 November 2025). Bruxelles: European Board for Digital Services / Commissione europea.
https://cdn.table.media/assets/europe/first_article_352_dsa_report_on_systemic_risks_and_mitigations_final_ddxkzxhwga8vftj3unr0mgkwqvk_121707.pdf
Fletcher, R., & Nielsen, R. K. (2018). Are people incidentally exposed to news on social media? A comparative analysis. New Media & Society, 20(7), 2450–2468.
Floridi, L. (2002). What is the philosophy of information? Metaphilosophy, 33(1–2), 123–145.
Gagliardone, I. (2019). Defining online hate and its "public lives": What is the place for "extreme speech"? International Journal of Communication, 13, 20.
Gebru, T., Morgenstern, J., Vecchione, B., Vaughan, J. W., Wallach, H., Daumé III, H., & Crawford, K. (2021). Datasheets for datasets. Communications of the ACM, 64(12), 86–92.
Guo, K., Hu, A., Mu, J., Shi, Z., Zhao, Z., Vishwamitra, N., & Hu, H. (2023). An investigation of large language models for real-world hate speech detection. In 2023 International Conference on Machine Learning and Applications (ICMLA) (pp. 1568–1573). IEEE.
Online Hate Working Group (2021). Online hate. Final report (5 February 2021).
Harriger, J. A., Evans, J. A., Thompson, J. K., & Tylka, T. L. (2022). The dangers of the rabbit hole: Reflections on social media as a portal into a distorted world of edited bodies and eating disorder risk and the role of algorithms. Body Image, 41, 292–297.
Hargittai, E. (2010). Digital Na(t)ives? Variation in Internet skills and uses among members of the "Net Generation". Sociological Inquiry, 80(1), 92–113.
Huang, L., Yu, W., Ma, W., Zhong, W., Feng, Z., Wang, H., & Liu, T. (2025). A survey on hallucination in large language models: Principles, taxonomy, challenges, and open questions. ACM Transactions on Information Systems, 43(2), 1–55.
Jane, E. A. (2014). "You're a ugly, whorish, slut": Understanding e-bile. Feminist Media Studies, 14(4), 531–546.
Khan, A. A., Laghari, A. A., Inam, S. A., Ullah, S., Shahzad, M., & Syed, D. (2025). A survey on multimedia-enabled deepfake detection: State-of-the-art tools and techniques,

emerging trends, current challenges & limitations, and future directions. Discover Computing, 28(1), 48.

Kosmyna, N., Hauptmann, E., Yuan, Y. T., Situ, J., Liao, X.-H., Beresnitzky, A. V., & Maes, P. (2025). Your brain on ChatGPT: Accumulation of cognitive debt when using an AI assistant for essay writing task. arXiv:2506.08872.

Knight-Georgetown Institute (2025). Systemic Risk Assessment under the Digital Services Act (Commentary, 15 May 2025). https://kgi.georgetown.edu/research-and-commentary/systemic-risk-assessment-under-the-digital-services-act/

Kroll, J. A., Huey, J., Barocas, S., Felten, E. W., Reidenberg, J. R., Robinson, D. G., & Yu, H. (2017). Accountable algorithms. University of Pennsylvania Law Review, 165(3), 633–705.

Matz, S. C., Kosinski, M., Nave, G., & Stillwell, D. J. (2017). Psychological targeting as an effective approach to digital mass persuasion. Proceedings of the National Academy of Sciences, 114(48), 12714–12719.

Mitchell, M., Wu, S., Zaldivar, A., Barnes, P., Vasserman, L., Hutchinson, B., Spitzer, E., Raji, I. D., & Gebru, T. (2019). Model cards for model reporting. In Proceedings of the Conference on Fairness, Accountability, and Transparency (FAT*) (pp. 220–229). ACM.

Papacharissi, Z. (2004). Democracy online: Civility, politeness, and the democratic potential of online political discussion groups. New Media & Society, 6(2), 259–283.

Pei, G., Zhang, J., Hu, M., Zhang, Z., Wang, C., Wu, Y., & Tao, D. (2024). Deepfake generation and detection: A benchmark and survey. arXiv:2403.17881.

Popan, J. R., Coursey, L., Acosta, J., & Kenworthy, J. (2019). Testing the effects of incivility during internet political discussion on perceptions of rational argument and evaluations of a political outgroup. Computers in Human Behavior, 96, 123–132.

Risko, E. F., & Gilbert, S. J. (2016). Cognitive offloading. Trends in Cognitive Sciences, 20(9), 676–688.

Roy, S., Harshvardhan, A., Mukherjee, A., & Saha, P. (2023). Probing LLMs for hate speech detection: Strengths and vulnerabilities. In Findings of the Association for Computational Linguistics: EMNLP 2023 (pp. 6116–6128).

Şahin, E., Arslan, N. N., & Özdemir, D. (2025). Unlocking the black box: An in-depth review on interpretability, explainability, and reliability in deep learning. Neural Computing and Applications, 37(2), 859–965.

Salvi, F., Horta Ribeiro, M., Gallotti, R., & West, R. (2025). On the conversational persuasiveness of GPT-4. Nature Human Behaviour, 9(8), 1645–1653.

Schiff, K. J., Schiff, D. S., & Bueno, N. S. (2025). The liar's dividend: Can politicians claim misinformation to evade accountability? American Political Science Review, 119(1), 71–90.

Suler, J. (2004). The online disinhibition effect. CyberPsychology & Behavior, 7(3), 321–326.

Suchman, L. A. (2007). Human–Machine Reconfigurations: Plans and Situated Actions. Cambridge: Cambridge University Press.

Tufekci, Z. (2015). Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency. Colorado Technology Law Journal, 13, 203–218.

Vaccari, C., & Chadwick, A. (2020). Deepfakes and disinformation: Exploring the impact of synthetic political video on deception, uncertainty, and trust in news. Social Media + Society, 6(1).

Wardle, C., & Derakhshan, H. (2017). Information disorder: Toward an interdisciplinary framework for research and policy making. Strasbourg: Council of Europe.

Woolley, S. C., & Howard, P. N. (2016). Political communication, computational propaganda, and autonomous agents: Introduction. International Journal of Communication, 10.

Yakura, H., Lopez-Lopez, E., Brinkmann, L., Serna, I., Gupta, P., Soraperra, I., & Rahwan, I. (2024). Empirical evidence of Large Language Model's influence on human spoken communication. arXiv:2409.01754.

Zhang, B., Cui, H., Nguyen, V., & Whitty, M. (2025). Audio deepfake detection: What has been achieved and what lies ahead. Sensors, 25(7), 1989.

Zuboff, S. (2023). Surveillance capitalism. The future of humanity in the age of new powers. Rome: Luiss University Press.

Zuiderveen Borgesius, F., Möller, J., Kruikemeier, S., Ó Fathaigh, R., Irion, K., Dobber, T., & de Vreese, C. H. (2018). Online political microtargeting: Promises and threats for democracy. Utrecht Law Review, 14(1), 82–96.

6 Copyright protection in the age of ChatGPT – what role for AGCOM?

Giuseppe Cassano

Summary: 1. Introduction. - 2. Technical evolution and copyright. - 3. AI-generated works and copyright. - 4. AI and visual information. - 5. The artificial author: was it truly an author? - 6. Comparative regulatory experiences. - 7. The object of copyright protection in the age of AI. - 8. AI and the amendments introduced by the legislator. - 9. Training of AI systems and copyright protection. - 10. Code of Good Practice for AI

6.1 Introduction

AGCOM has a primary role in the protection of copyright, as the legislator itself has repeatedly recognised over the years (see Law No. 633 of 22 April 1941; Legislative Decree No. 70 of 9 April 2003; Legislative Decree No. 35 of 15 March 2017; Legislative Decree No. 208 of 8 November 2021).

Most recently, the following should be noted:

- Legislative Decree No. 177 of 8 November 2021 (implementation of Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market), according to which, two years after the date of entry into force of that decree, the Italian Communications Regulatory Authority shall submit to Parliament a report, supplemented by a regulatory impact assessment, on the application of the provisions falling within its competence, with particular reference to the criteria and methods for determining fair compensation for press publishers under Article 43-bis of Law No. 633 of 22 April 1941, and to the procedure for determining remuneration for authors, artists, performers and executants, following consultation with collective management organisations or independent management entities under Legislative Decree No. 35 of 15 March 2017 (Article 2);

- Law No. 93 of 14 July 2023 (Provisions for the prevention and repression of the unlawful dissemination of copyright-protected content through electronic communications networks), under which, among other things, AGCOM, by its own order, requires service providers, including access providers, to disable access to unlawfully disseminated content by blocking DNS resolution of domain names and blocking the routing of network traffic to IP addresses primarily intended for unlawful activities (paragraph 1). The same order also requires the blocking of any future domain name, subdomain or IP address, attributable to anyone, including variations of the name or of its simple declension or extension (so-called top-level domain), allowing access to the same unlawfully disseminated content and to content of the same nature (paragraph 2).

To close this brief summary of the relevant regulatory framework, it is useful to recall the Regulation of the European Parliament on a single market for digital services — the Digital Services Act (DSA) — according to which Member States designate one or more competent authorities responsible for supervising providers of intermediary services and enforcing the Regulation (Article 49).

The Italian Communications Regulatory Authority has been designated as Digital Services Coordinator (Article 15 of Decree-Law No. 123 of 15 September 2023 — urgent measures to combat youth distress, educational poverty and juvenile crime, and to protect minors in the digital environment — converted into law, with amendments, by Article 1(1) of Law No. 159 of 13 November 2023).

6.2 Technical evolution and copyright

The ceaseless, unstoppable and almost authoritarian spread of Artificial Intelligence (AI) in the everyday life of individuals, businesses and public actors opens new frontiers of debate on copyright protection. This could not be otherwise, since every major technical evolution has always been matched by the need to reshape the protection at issue here (Adelaide Rossi).

The relationship between technical evolution and copyright is therefore not a topic exclusive to our own time, nor one typically belonging only to generative artificial intelligence (also referred to here as GenAI).

By "generative artificial intelligence" is meant the field of artificial intelligence that focuses on creating new and original content, compared with input data, in response to user requests (prompts), through the use mainly of neural algorithms.
By "neural network" is meant a standard computational model applicable in highly diverse contexts, allowing recognition of objects, shapes or patterns within a datum or set of data, such as a human face in a photograph.
Generative artificial-intelligence algorithms are used in a wide range of applications, including recognition and generation of images, voice or music tracks, texts and videos (Italian Data Protection Authority, Order No. 232 of 10 April 2025).

6.3 AI-generated works and copyright

Over time, copyright protection has already been debated with regard to photography, databases (CJEU, Third Chamber, 18 October 2012, Case C-173/11), software, technical projects (most recently TAR Emilia-Romagna, Bologna, Section I, 22 October 2025, No. 1180), and so forth, reaching solutions that may still be useful in relation to AI.
With regard to photography, the teaching of the CJEU (Third Chamber, 1 December 2011, Case C-145/10) remains valid: a photographic portrait may be protected by copyright if, as the national court must verify case by case, it constitutes the author's intellectual creation, reflecting the author's personality and expressed through free and creative choices in making that portrait.
Precisely in relation to a photograph, Italy saw one of the first decisions of the Supreme Court of Cassation concerning software and copyright protection for a work generated with AI.
The matter began with the claim by the creator of the graphic work "The Scent of the Night", seeking a finding of infringement of her copyright and an order against the defendant (RAI) to pay damages for the unauthorised use of that work as fixed scenography at the 2016 Sanremo Festival.
The first-instance court (Court of Genoa, judgment No. 1640 of 6 June 2018) upheld the claim, and that decision survived review on appeal (Court of Appeal of Genoa, specialised business section, judgment No. 1066 of 11 November 2020).
Ultimately, the Court of Cassation, by order No. 1107 of 16 January 2023, although addressing the issue only incidentally, nevertheless gave the green light to the

possibility of attributing creative character to a photograph made by its author using AI software.

According to the Supreme Court, the admission that software had been used to generate the image is a circumstance still compatible with the creation of an intellectual work having a degree of creativity, to be scrutinised only with greater rigour.

6.4 AI and visual information

Image-generating GenAI is a frontier towards which one should move while governing the controversial issues it raises and, at the same time, taking advantage of its many useful applications for individuals and society.

After all, it cannot seriously be disputed that knowing and understanding is essential before deciding whether and how to use the tool.

Although everyone has recently been talking about Artificial Intelligence — divided more or less equally between those who approach AI with utopian optimism and those who approach it with greater fear and distrust — few truly know what they are talking about.

Even scholars in the humanities who approach AI — and lawyers plainly fall within this category — often find themselves in a true cognitive deficit: they discuss an object largely unknown to them, a sort of UFO, one might say (Diana-Urania Galetta).

A certainly useful application of image-generating GenAI for the community can be found in artificial vision applied to the reconstruction of visual artefacts, such as ancient frescoes, pictorial surfaces, fragmentary or deteriorated paintings, in order to recognise chromatic patterns, textures, material traces, missing portions and stratifications of the individual works examined.

Computer-vision techniques make it possible to reconstruct lost parts, suggest plausible integrations, identify later pictorial layers, classify pigments or detect previous restoration interventions. The goal becomes the reconstruction of the image, the understanding of its visual structure and the most faithful possible restitution of the artefact's original appearance.

This contributes to the enhancement and study of cultural heritage, the so-called artificial intelligence applied to cultural assets.

Here AI is called upon to operate exclusively on visual information: to analyse shapes, colours, textures and patterns in order to identify damaged parts, improve the legibility of surfaces or propose plausible reconstructions of missing areas. It is therefore work centred on image processing and requiring technical and IT skills: computer vision, generative models and visual segmentation (TAR Campania, Naples, Section V, 5 March 2026, No. 1525).

6.5 The artificial author: was it truly an author?

The many questions that legal practitioners are now called upon to address in the relationship between generative AI and copyright require broad solutions that go beyond the path traced by national regulatory experiences as shaped over the years by case law; GenAI, in particular, requires rethinking the coordinates describing the subjects and object of the right.

As regards the subjective profile of protection, GenAI raises the question whether it is possible to configure a sort of "artificial" author.

A preliminary consideration is appropriate. The relevant regulatory framework — national, EU and international — is not decisive, because sometimes it refers to the author as a natural person, at other times it admits the author as a legal person, but never goes so far as to grant protection to an artificial author.

At the same time, several factors point towards limiting authorship to natural persons, or within certain limits to legal persons, thereby neutralising and eliminating the issue of the artificial author.

Indeed, it is with reference to the human person that the legislator grants, in the event of proven infringements, protection also of moral rights; and it is only with reference to the human person that one can speak of death in this field, which is relevant for calculating the duration of protection.

Finally, and importantly, the author makes conscious choices when creating a work, whereas no consciousness can be attributed to AI systems.

Nor can one omit a reference to Article 27 of the Universal Declaration of Human Rights, according to which everyone has the right freely to participate in the cultural life of the community, to enjoy the arts and to share in scientific advancement and its benefits, and everyone has the right to the protection of the moral and material

interests resulting from any scientific, literary or artistic production of which he or she is the author.

It is therefore beyond doubt that one cannot speak of human rights in relation to a machine which, to remain within the topic at hand, is not conscious, does not suffer, does not feel emotions capable of grounding non-pecuniary rights protection, and will never die, but at most cease functioning.

6.6 Comparative regulatory experiences

The issue just outlined calls for reflection in light of the legislation in force in countries even far from ours, which may nevertheless offer useful insights to be considered with interest. As noted from the outset, the subject requires solutions as homogeneous as possible and capable of going beyond national borders.

The first reference is Article 11 of the Chinese copyright law, which clearly identifies only the natural person who created the intellectual work as its author, thus excluding any interpretation that would include an artificial author within that concept.

More precisely, the provision states: "An author is a natural person who creates a work. The author is the natural person who creates the work. For works hosted by a corporate or unincorporated organization, created on behalf of the will of the corporate or unincorporated organization, and for which the corporate or unincorporated organization assumes responsibility, the corporate or unincorporated organization shall be regarded as the author".

The merely auxiliary role that the GenAI system must perform therefore emerges. For a judicial application of this legislation, reference may be made to the judgment of the Beijing Internet Court of 27 November 2023, No. 11279, which imposed liability for the unlawful use of an image generated by Stable Diffusion (Virgilio D'Antonio - Ciro Maria Ruocco).

In the US regulatory experience, both the Copyright Act and, even more clearly, the Compendium of U.S. Copyright Office Practices deny protection to works resulting solely from mechanical processes.

Still looking at the US experience, it is useful to recall the guidelines of the U.S. Copyright Office of 16 March 2023, which clarified that copyright protects only works created by humans, noting that public guidance is needed on registration of works

containing AI-generated content and explaining how the Office applies the human authorship requirement to such applications.

At the same time, the Office specified that its policy statement sets out the approach to registration of works containing material generated by AI technology, while it will continue to monitor factual and legal developments and may issue further guidance in the future.

As for the Mexican system, reference should be made to the Federal Law of Author's Right (Ley Federal del Derecho de Autor - LFDA), which places the natural person at the centre of protection.

Recently, the decision of the Supreme Court of Justice of the Nation of Mexico, Second Chamber, judgment of 2 July 2025, Amparo Directo 6/2025, emphasised the anthropocentric dimension of copyright, excluding any possible recognition of authorial status for artificial-intelligence systems (Virgilio D'Antonio - Ciro Maria Ruocco).

Turning now to the old continent, it should be noted that UK legislation differs considerably from continental legislation (Ciro Maria Ruocco).

Section 178 of the Copyright, Designs and Patents Act 1988 provides, among other minor definitions, that "computer-generated", in relation to a work, means that the work is generated by computer in circumstances such that there is no human author of the work; the reference to a work generated by computer in the absence of a human author is clear.

Strictly speaking, this rule refers to ordinary computers rather than intelligent machines, but its scope is now extended to the latter as well.

As regards authorship of works created by such machines, section 9(3) provides some assistance, although it does not resolve all interpretative issues: in the case of a literary, dramatic, musical or artistic work which is computer-generated, the author is taken to be the person by whom the arrangements necessary for creation of the work are undertaken. Thus, the author is the person who makes the necessary arrangements for creation.

Mention must also be made of Article 15 of the Berne Convention for the Protection of Literary and Artistic Works, ratified and implemented in Italy by Law No. 399 of 20

June 1978, which provides that, in order for authors of protected works to be regarded as such until proof to the contrary and admitted to bring proceedings before the courts of Union countries, it is sufficient for the author's name to appear on the work in the usual manner. This provision assumes — as was obvious when it was signed on 9 September 1886 — that the author is a natural person.

Finally, with regard to the EU experience, the following should be considered:

- Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases (the Database Directive), according to which the author of a database is the natural person or group of natural persons who created it, or, where the legislation of the Member State concerned so permits, the legal person designated as rights holder by that legislation (Article 4(1));
- Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (the Software Directive), according to which protection is granted to all natural or legal persons eligible under national copyright law as applied to literary works (Article 3).

It follows that, according to the European legislator, the author of a database or software may be a natural person, a group of natural persons and, where national legislation allows, also the legal person that created the program.

6.7 The object of copyright protection in the age of AI

Turning now to the objective profile of copyright protection in the age of AI, some reference must be made to the constituent elements of that right.

According to settled case law, copyright protection requires originality and creativity. These may exist even where the work is composed of simple ideas and notions included in the intellectual heritage of persons experienced in the relevant field, provided they are formulated and organised in a personal and autonomous manner compared with previous works (Court of Cassation, 13 June 2014, No. 13524; 28 November 2011, No. 25173; 12 March 2004, No. 5089; 2 December 1993, No. 11953). In particular, creativity lies not in the idea underlying the work, but in the form of its expression, that is, in its subjectivity. The same idea may underlie several works, as often happens with artistic works, which may differ because of the subjective creativity

spent by each author, and that is what matters for obtaining protection (Court of Cassation, 29 May 2020, No. 10300).

These legal principles, stated by national case law (most recently Court of Cassation, First Section, order No. 3393 of 10 February 2025), conform to the principles developed on the matter by the CJEU.

According to the CJEU, starting from Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001, the concept of a work implies the existence of an original subject matter, in the sense that it represents the author's own intellectual creation, while the classification as a work is reserved to elements that are the expression of that creation (CJEU 12 September 2019, Cofemel, C-683/17, paragraph 29; CJEU 13 November 2018, Levola Hengelo, C-310/17, paragraphs 33 and 35 to 37).

For a subject matter to be regarded as original, it is necessary and sufficient that it reflect the personality of its author, by expressing the author's free and creative choices. The concept of work also necessarily implies the existence of subject matter identifiable with sufficient precision and objectivity (CJEU 12 September 2019, Cofemel; CJEU 13 November 2018, Levola Hengelo).

Furthermore, Articles 2 to 5 of Directive 2001/29 must be interpreted as meaning that copyright protection applies to a product whose form is at least partly necessary to obtain a technical result, where that product constitutes an original work resulting from intellectual creation because, through that form, the author expresses creative ability in an original manner by making free and creative choices, so that the form reflects the author's personality; this is for the referring court to verify in light of all relevant elements (CJEU, Fifth Chamber, 11 June 2020, Case C-833/18).

Finally, in this field infringement does not occur only when a work is copied in full, namely through unlawful reproduction, but also in cases of counterfeiting, which occurs when the essential features of the earlier work recur in the later one.

Those essential features of the work, which therefore cannot be replicated, must be identified by reference to what is the product of the author's creativity. What matters is the expressive form in its subjectivity, namely the author's choice in representing the idea, and not the idea as such (Court of Cassation, First Section, order No. 21851 of 29 July 2025).

6.8 AI and the amendments introduced by the legislator

In light of the above, it is now necessary to analyse the legislation following the interventions aimed at regulating the relationship between copyright on the one hand and GenAI on the other.

First, Article 1 of Law No. 633/1941, as amended by Law No. 132 of 23 September 2025 on artificial intelligence, should be recalled: it provides that works of human intellect having creative character and belonging to literature, music, figurative arts, architecture, theatre and cinema are protected, whatever their mode or form of expression, including where created with the aid of artificial-intelligence tools, provided that they constitute the result of the author's intellectual work (paragraph 1).

The 2025 legislator — curiously without also amending Article 2575 of the Civil Code — thus grants protection to works created with the aid of AI tools, while making clear that the fixed point is, and must remain, the result of the author's intellectual work.

The perspective is therefore anthropocentric, as it had to be, since the entire system of Law No. 132 is marked by an anthropocentric dimension of artificial intelligence (Article 1).

Article 1 of Law No. 633 therefore shows that, with regard to the topic addressed here, no new issues arise either for works resulting exclusively from human contribution, since they do not interact with GenAI systems, or for works resulting exclusively from AI contribution, since such works are excluded by the statutory framework, AI tools being only auxiliary.

Copyright can and must instead be discussed with regard to works resulting from human contribution that makes use of GenAI, a right that requires shared and homogeneous solutions at least at European level.

Let us look more closely at the issues to be resolved.

More precisely, the issue concerns the legal relevance, from the standpoint of copyright protection, of the input, that is, the data used to train the AI system.

As for the output, namely the work generated by the AI system, if it is entirely the product of an artificial author it falls outside the scheme of legal protection; if it is a work created by a human author with the aid of an AI system, protection will follow ordinary routes.

6.9 Training of AI systems and copyright protection

As is well known, image-generating AI capable of producing original images — and easily accessible also because of often relatively low costs — requires legal practitioners to analyse the legal relevance of a user entering a prompt, that is, a text, into a deep-learning system to create a new and unprecedented image.

Generative AI needs to draw on a very large amount of information, in the order of billions of items, for its learning, and it often also draws on copyright-protected works, raising the issue of protection of copyright, for which different regulatory solutions exist.

Thus, while the United States relies on the principle of fair use, governed by U.S. Copyright Law, Chapter 1, Section 107, which permits incorporation of copyrighted material in works for criticism, teaching, research and journalism, the EU experience is based on the exception for Text and Data Mining (TDM).

In Italy, in particular, Article 70(1-bis) of Law No. 633/1941 expressly allows free publication on the internet, without charge, of low-resolution or degraded images and music for teaching or scientific use and only where such use is not for profit; the limits of teaching or scientific use are to be defined by ministerial decree after the required consultations.

Article 70-ter allows reproductions made by research organisations and cultural-heritage institutions for scientific research purposes, for text and data mining from works or other materials available in networks or databases to which they have lawful access, as well as communication to the public of research results where expressed in new original works.

Article 70-quater provides that, without prejudice to Article 70-ter, reproductions and extractions from works or other materials contained in networks or databases to which one has lawful access are permitted for text and data mining, where use of the works and materials has not been expressly reserved by copyright holders, holders of related rights or database rights holders.

Finally, Article 70-septies provides that, without prejudice to the Berne Convention, reproductions and extractions from works or other materials contained online or in databases to which one has lawful access, for text and data mining through artificial-

intelligence models and systems, including generative systems, are permitted in accordance with Articles 70-ter and 70-quater.

This last provision, introduced by Article 25(1)(b) of Law No. 132/2025, expressly incorporates the rules on text and data mining into Law No. 633/1941, demonstrating the legislator's intention to protect the training needs of artificial-intelligence systems. Its most immediate reference is Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence, particularly Article 53 on obligations for providers of general-purpose AI models, although comparison of the two texts shows that Article 53, unlike the Italian text, does not refer to text and data mining, which is instead mentioned in recital 105.

It follows that training AI systems and models on copyright-protected material is lawful, thanks to the text and data mining exception, provided that the material is lawfully accessible and that the rights holder has not exercised opt-out. The methods for exercising that option, and the issue of liability in case of non-compliance, remain to be clarified (Bruno Tassone – Sara Manni). The matter is objectively more complex and can be better understood through the issues addressed by the Munich Regional Court.

More specifically, on 11 November 2025 the Munich I Regional Court (Landgericht München I) ruled against OpenAI in the case brought by the German collecting society GEMA.

The court held in particular that the platform's use of song lyrics infringed copyright:

Ø by storing song lyrics

Ø by displaying parts of the lyrics in the output.

The court therefore held that the text-and-data-mining limitation under Article 4 of Directive 2019/790 did not apply, because those lyrics, being contained in the model parameters and capable of being returned as output, were not merely used for analytical purposes but stored in the strict sense, that is, incorporated in a stable and reusable manner.

This phenomenon of storage marks the dividing line from the mere extraction of text and data that characterises text and data mining.

Storage occurs when, during training, language models not only extract information from the training dataset but also show complete incorporation of training data into the specified parameters after training, so that song lyrics are also reproduced in outputs.

The court distinguished between:

• merely preparatory reproductions necessary for data analysis

• reproductions that result in stable incorporation of the work into the model.

In the first case, the law permits temporary reproduction because it is functional to subsequent analysis.

In the second case, however, permanent reproduction affects the author's economic exploitation rights.

Accordingly, the Munich Regional Court, by judgment of 11 November 2025 - 42 O 14139/24, ordered OpenAI USA and OpenAI Ireland to cease:

• reproducing, in whole or in part, without GEMA's consent, the song lyrics attached in file K1 within language models (Large Language Models) and/or causing third parties to perform such acts;

• making publicly accessible and/or reproducing, in whole or in part and/or in the form of adaptations, without the claimant's consent, the song lyrics attached in file K1 in the outputs of a chatbot, and/or causing third parties to perform such acts (file K2).

The defendants were also ordered to provide the claimant with information on the extent of the conduct described and the revenues derived from it, indicating:

• the number and extent of the acts;

• the revenues for each defendant.

It was also declared that the defendants are obliged to compensate the claimant for all damage already suffered and/or to be suffered as a result of the conduct described in point 1, according to the information provided under point 2.

We are therefore facing new challenges and a criterion of reference already well known: the three-step test under Article 9(2) of the Berne Convention and Article 5 of Directive 2001/29/EC, according to which exceptions and limitations to copyright are allowed only under the following conditions:

• Special case

The use falls within a clearly defined and circumscribed exception.

• No conflict with normal exploitation of the work

The exception must not compromise the current or potential market for the work.

• No unjustified prejudice to the legitimate interests of the rights holder

The impact on the author's rights must remain proportionate and reasonable.

All this without forgetting that exceptions and limitations cannot be applied in such a way as to prejudice the legitimate interests of rights holders or conflict with normal economic exploitation of their works or protected materials. It may therefore be necessary further to limit the scope of certain exceptions or limitations in the case of some new uses of works and protected materials (recital 44).

Code of Good Practice for AI

6.10 Providers of generative artificial-intelligence models must finally comply with the Code of Good Practice for AI (CPAI), according to which, among other things, they expressly commit as follows:

In order to help ensure that Signatories will identify and comply with, including through state-of-the-art technologies, machine-readable reservations of rights expressed pursuant to Article 4(3) of Directive (EU) 2019/790 if they use web-crawlers or have such web-crawlers used on their behalf to scrape or otherwise compile data for the purpose of text and data mining as defined in Article 2(2) of Directive (EU) 2019/790 and the training of their general-purpose AI models, Signatories commit:

a) to employ web-crawlers that read and follow instructions expressed in accordance with the Robot Exclusion Protocol (robots.txt), as specified in IETF Request for Comments No. 9309 and any subsequent version technically feasible and implementable by AI providers and content providers, including rightsholders; and

b) to identify and comply with other appropriate machine-readable protocols for expressing rights reservations under Article 4(3) of Directive (EU) 2019/790, for example through asset-based or location-based metadata, adopted by standardisation bodies or representing the state of the art, technically implementable and widely

adopted by rightsholders, considering different cultural sectors and agreed through an inclusive process at EU level.

In summary, where providers that are signatories to the Code use web crawlers, or have them used on their behalf, to extract or compile data for text and data mining and for training general-purpose AI models, they must commit to:

a) using web crawlers that read and follow instructions expressed in accordance with the Robot Exclusion Protocol (robots.txt);

b) identifying and respecting other appropriate machine-readable protocols to express rights or reservations under Article 4(3) of Directive (EU) 2019/790.

Finally, a criminal penalty applies to anyone who reproduces or extracts text or data from works or other materials available online or in databases in breach of Articles 70-ter and 70-quater, including through artificial-intelligence systems (Article 171 of Law No. 633/1941, as amended by Law No. 132/2025).

For a recent practical application of the above, reference may be made to the judgment of the Hamburg Regional Court (Landgericht Hamburg, Civil Chamber 10, Case No. 310 O 227/23, delivered on 27 September 2024), which addressed the lawfulness of collecting copyright-protected works to create datasets for training AI systems and held that such activity was lawful in that case when carried out by a non-profit organisation. The decision is based on § 60d UrhG, implementing Article 3 of Directive 2019/790 (Ciro Maria Ruocco - Vera Iuzzolino).

Reference should also be made to the already cited judgment of the Munich I Regional Court (Landgericht München I, 42nd Civil Chamber, judgment of 11 November 2025, Case No. 42 O 14139/24), which concerns the use of copyright-protected song lyrics for training and operation of GenAI models and denies, in that case, reliance on the text and data mining exception.

7 AI and the education of young people

Mauro Giusto

7.1 The paradox of the most connected but least aware generation

Today's young people (aged 10 to 25) are the first who do not remember a world without algorithms, voice assistants, or personalised feeds selecting reality for them. In Italy and Europe, the use of generative AI among children and adolescents is close to 90% in the 9–16 age group. Yet they are also the generation that least understands the mechanisms governing it. They use the tools, but do not know who is using them through those tools.

This lack of awareness is not merely a technical problem: it is a fundamental anthropological, political and, above all, ethical issue. It is precisely the starting point of the reflection of Father Paolo Benanti, Franciscan, theologian and professor of Ethics of Technology at the Pontifical Gregorian University, chair of the Italian Government's AI Commission for Information, the only Italian member of the UN Committee on Artificial Intelligence and adviser to the last two Popes on these matters. His position is very clear and at the same time disruptive: the problem is not the machine as such. The real problem is leaving young people alone in front of that instrument and its dynamics.

If we immerse them in the digital world outside meaningful human relationships, we have already implicitly decided that we are not truly interested in educating them.

Around this conviction, in recent years, a constellation of thinkers, institutions and educational experiences has formed around one central point: artificial intelligence cannot be separated from ethics, and young people cannot be left without the means to understand it and inhabit it freely and responsibly.

7.2 It is not only technology: it is a transformation of the human

The first mistake to avoid when speaking about AI and young people is reducing the matter to a technical issue — skills, computer literacy and coding. The artificial-

intelligence revolution is not only technological; it is an anthropological, cultural and sociological transformation. It does not affect only what young people do, but changes what they are and how they perceive themselves: how they build their identity, relate to others, learn, feel emotions and imagine their own future and the future of the world. To understand the scope of this change, let us return to Father Benanti's thought. There is a new and well-defined philosophical category: the techno-human species. Human beings have never faced the world bare-handed. For tens of thousands of years, they have modified it through the ideas they can implement — fire, writing, printing, steam, electricity, the digital — and these artefacts, in turn, transform human beings themselves. Technology cannot be neutral: it carries with it a view of the universe, values, a set of powers and risks. Every new tool changes the boundaries of what is possible and, in doing so, changes those who know how to use it.

This thought, deeply rooted in the philosophy of technology, beginning with Aristotle, finds its most radical current embodiment in the figure of the algorithm. An algorithm is not simply computer code: it is a disposition of power and a form of order. Every AI system entering a social context redistributes visibility, access, hierarchies and opportunities. The visibility of a piece of content, an opinion, a candidate or a product no longer depends only on its quality or merit, but on the position assigned to it by the algorithm. This is a power that, in most cases, acts invisibly to its own users and is therefore particularly insidious towards younger human beings, who do not yet have the tools to recognise it.

Young people are immersed in this power from childhood, and the education system does not reveal to them its risks as well as its potential.

7.3 An ethical compass is needed to navigate the world of algorithms

There is now a neologism that has entered the international vocabulary: algorethics (Benanti). The word was born from the fusion of algorithm and ethics, and is recognised by the Accademia della Crusca and adopted by the UN in its own terminology. It arises from a simple but alarming observation: if a machine can decide whether to grant or deny a mortgage, if an algorithm can orient sentencing in criminal

proceedings, if an automated system can select the information a young person receives every day and silently shape their worldview, then that machine is not simply executing code. In this case, it acts on ethical values produced by human beings, and those values must be made computable consciously and responsibly, not hidden.

Algorethics does not attribute moral consciousness to the machine: the machine is not an ethical subject. It recognises that algorithmic systems incorporate values, criteria and hierarchies chosen — more or less consciously — by human beings. Whenever an algorithm chooses what to show a fourteen-year-old, it is making a value choice: what is relevant, what is desirable, what is normal. And that choice has been made by someone who, very often, is not the adolescent, nor their family or school, but a technology corporation that primarily responds to its own profit logic.

For this reason, algorethics, according to many, is no longer only a matter for engineers and experts: it is a citizenship competence that must be taught from school onwards, with the precise aim of preventing every individual — and especially every young person — from giving up their critical conscience by allowing the machine to act on their behalf, thereby losing the meaning of what they do and what they are.

7.4 Educational abandonment

The machine, therefore, is not the enemy. The real problem is educational abandonment: leaving young people alone in front of tools of unprecedented power, in the absence of adults capable of accompanying them in this encounter.

A machine that always agrees, always answers, never tires, never argues and never gets angry is an endless temptation for an adolescent building their identity and seeking confirmation. But this temptation becomes a trap when there is no one — parent or educator — helping the young person understand what they are really seeking, or why they are seeking it in a technological system rather than in a human relationship.

The real question is why a young person does not have someone with whom to engage. The issue is that a minor in the midst of growth finds in AI answers the only available source. Clearly, this is not a matter of technology, but of the role and responsibilities of adults.

Problems of relationship and growth are not solved through rules. They belong to an exclusively human space that adults must fully share with younger people. This

requires effort, dedication and commitment. When this does not happen, young people risk paying dearly, and alone, for the presence that adults fail to provide.

7.5 The machine always answers: risks for identity

Generative AI enters the lives of minors at the most delicate moment of their development, when identity is being formed.

Adolescence is by nature the time of conflict, confrontation, acceptance and rejection. It is the moment in which one learns to manage failure, negotiate perspectives different from one's original ones, and develop resilience and empathy through real relationships. Human relationships involve complexity and conflict, and through these passages the person's character is formed. It is a complicated but necessary path.

An AI system, as it is conceived, tends to do the opposite: it accommodates, confirms, adapts to the user and offers unconditional acceptance. It never exposes the user to rejection. It never causes discomfort or exclusion. It never presents confrontation with a reality that resists. For a fragile adolescent, this may seem a very easy path. In fact, however, it deprives them of the experience of limits, which is indispensable for psychological maturation.

Experts call algorithmic subjectivation the process by which young people internalise algorithmic criteria of value — likes, scores, visibility — and use them to construct their public self. Identity is therefore no longer formed only through encounters with other human beings, but through continuous dialogue with artificial agents that shape subjectivity, filter experience and return an always confirming and reassuring image of who one already is. The result may unfortunately be a self-referential identity, unable to withstand confrontation with reality and its inevitable resistance, which is necessary for growth.

In increasingly frequent cases, some young people develop what psychology calls a "surrogate affective relationship" with machines, attributing to them human qualities such as mutual respect, empathy and deep understanding. It is a perfect seduction and therefore very dangerous, because it distances them from the indispensable risk of real relationships. But what is the long-term result if a young person constructs their idea of the other through a system that never makes mistakes, never gets tired and never shows its fragilities? They will grow up seeking "perfect" interlocutors in the real

world, unable to tolerate the structural imperfection of every authentic human relationship.

7.6 The deepfake challenge: AGCOM's role

To this is added an equally risky political dimension: artificial intelligence, through search engines, recommendation systems and personalised social-media feeds, does not merely dialogue with young people; it forms them. It shapes their worldview, their opinions and the boundary between what they consider normal and what they consider unacceptable.

This is what Benanti has called sharp power, namely AI's ability to modify behaviours without explicitly changing ideas. Digital propaganda conditions; it does not need to convince. It selects without arguing. It does not need to persuade openly, but constructs closed information environments — so-called echo chambers — in which certain viewpoints appear universal and others seem entirely absent. An adolescent living in an echo chamber does not realise it: their bubble will seem to them to be the world. This confusion between bubble and reality is one of the most serious risks for the construction of critical and democratic consciousness.

Adding to this the challenge of deepfakes — increasingly realistic synthetic images, videos and audio generated by AI systems — undermines the very ability to distinguish the real from the false. In this difficult challenge, an institutional actor such as AGCOM may have a decisive ethical and educational role, denouncing and stigmatising these distorting systems capable of further dismantling the backbone of correct communication. A community of citizens who can no longer distinguish an authentic document from an artificially constructed one risks rapidly becoming a place where democracy is seriously compromised.

7.7 The role of school

Faced with this scenario, schools are called upon to make a major qualitative leap that goes far beyond introducing coding into the curriculum or using tablets in class. This is a crucial challenge: forming young people capable of thinking critically about technology, questioning it instead of passively undergoing it, and recognising the implicit values it carries. Ultimately, they must consider it a tool.

Schools will have to increase young people's understanding of what artificial intelligence truly is, and this is a primary task of educational institutions. AI can be a highly effective tool for personalising learning and expanding teachers' ability to adapt to the specific needs of each student, making knowledge more accessible and inclusive and reducing some barriers that make learning unequal. But without an ethical vision and well-defined rules, the results could instead be exclusion, standardisation and profiling.

It should be borne in mind that the Guidelines of the Ministry of Education and Merit (2025) already recognise this urgency and identify three fundamental principles:

The human being at the centre — AI must remain at the service of the human person and not replace human responsibility; awareness — teachers and students must know algorithmic mechanisms in order to avoid passive or unaware use;

responsibility — those who use AI must answer for the adoption of their choices in terms of equity and educational impact.

Moreover, the European Artificial Intelligence Regulation (AI Act, 2024) moves in the same direction, classifying AI systems used in education as high-risk systems precisely because they can influence growth paths and life opportunities.

It nevertheless emerges that problems of growth and relationship are not only regulatory issues and cannot be solved through ministerial circulars or regulations, however well structured. What is actually required is a strong adult presence: parents, educators and teachers capable of accompanying young people also physically, not only through access to screens.

7.8 Educating for algorethics: learning to ask the right questions

Translating algorethics into educational practice requires working on several levels at the same time. It is necessary not to reduce everything either to technique alone or to abstract ethics alone.

Knowledge is the first level: understanding what an algorithm is, how it learns from data, who designs it and for what purpose, and who is responsible when it causes harm or inequality. Understanding the underlying mechanisms is necessary in order not to be naively subjected to their effects, and above all in order to ask the right questions in the right place.

Critical discernment is the second level: it consists in the ability to recognise profiling, echo chambers, emotional manipulation through personalised content and deepfakes. It means distinguishing genuine understanding from the simulation of understanding, and recognising when the machine is accommodating rather than
helping one to grow. In other words, it means understanding when the ease offered by AI is a gift and when it is a trap.

Responsibility and participation are the third level. Being active citizens in the construction of rules for AI, and not merely passive users, is essential in order to avoid the risks of passivity and manipulation. The central issue is knowing how to formulate the right questions in both form and content.

Recognising the irreplaceable value of human relationship is probably the central theme towards which the other levels must tend.

Indeed, understanding that what an algorithm can simulate — listening, empathy, understanding and presence — may not have the same nature when transposed into the real world is central to identifying what a human being truly is and what they need in order to grow well, beyond algorithms and machines.

7.9 Public governance. A political question

Among the most complex questions concerning AI and young people is the issue of age limits for access to platforms. It now seems clear that a limit is absolutely necessary. At the same time, the problem shifts to a more urgent level: who actually verifies the minor's age? Is it really possible to leave to large technology corporations the power to build a registry of all users even more detailed and pervasive than the public one?

It will be necessary to develop a system capable of verifying users' age without asking large private groups for real personal data that could endanger minors' protection and privacy. In other words, there must be transparent public control, potentially removed from the logic of profit. Here we return to a vision in which governance is more important than technique, and governance itself belongs to democratic States, not companies. No delegation to the market, therefore, for decisions concerning the future, education and identity of young people.

7.10 Conclusions for an aware approach to AI

A clarification: understanding how an algorithm works is necessary, but not sufficient.

The problem is not only cognitive; it is a matter of ethical education.

It is an existential and relational problem, affecting the way young people live in time, in relationships and within themselves.

Young people live in a time in which speed is an absolute value, answers are always immediate, waiting is perceived as a defect and silence as an absence to be filled. AI systems perfectly satisfy these times. Real life, however, is made of deep relationships, choices and growth through error and confrontation; it cannot be compressed.

A school that looks to algorethics must place education to slowness, questioning and productive doubt at the centre of its values.

Part of teaching must not be delegated to machines, not because machines are incapable, but because responsibility for those decisions belongs only to human beings. It identifies as indispensable the relationships between teacher and student, among peers and between generations. In this way, values are preserved that no algorithm will ever be able to replicate.

Keeping the person at the centre of reflection on AI does not mean being against technology, nor does it mean lamenting a non-return to the analogue world. It means remembering, insistently, that technology is made by human beings for human beings, and not the other way around. A school that educates with ethics at the centre of pedagogy gives young people not only skills, but questions and directions for reflection. Not only immediate answers, but the ability to encounter the other, knowing that no machine will ever be able to replicate that encounter.

Main sources: Paolo Benanti, Human in the Loop (LEV, 2018); Paolo Benanti and Sebastiano Maffettone, Noi e la macchina. Un'etica per l'era digitale (LUISS University Press, 2023); Rome Call for AI Ethics (Pontifical Academy for Life, 2020); UNESCO Recommendation on the Ethics of Artificial Intelligence (2021); Luciano Floridi, The Ethics of Artificial Intelligence (Oxford University Press, 2023); Ministry of Education and Merit, Guidelines for the introduction of AI in schools (2025); European Artificial Intelligence Regulation / AI Act (2024).

8 The Mosaic of Rules in the Digital Ecosystem*

Giovanna de Minico**

Summary: 1. Lines of reasoning. - 2. Technology defines the uncertain elements of anticompetitive conduct. - 3. Technology and digital markets. - 4. Technology from self-regulation to source of law. - 5. Conditions for the legitimacy of codes as sources. - 6. Do the codes under the DSA comply with the model of constitutional compatibility? - 7. The Artificial Intelligence Act and its claim to orient technology towards the human person. - 8. Technology as a "source of law". - 9. Looking to the future.

8.1 Lines of reasoning

Law and technology have met, intertwined and become confused in a mutable relationship that has allowed each to take the place previously occupied by the other, as made inevitable by the political dialectic expressed in that relationship, which never freezes its actors in predetermined positions.

The tension of technology towards human emancipation was already present in Aeschylus, who recounts Prometheus' theft of divine fire in order to free human beings from ignorance and allow them to compete with the gods.[15] Yet the fact that Prometheus dies chained to the rock of the Caucasus also shows the inability of technology to keep its original promise: to lead human beings to happiness.

Aristotle recovers Aeschylus' intuition, but develops it through autonomous means: he still preserves the aim of making human beings happy, yet pursues it through the dianoetic virtues — primarily ethics, wisdom and intellect.[16] These nourish politics,

** Full Professor of Constitutional and Public Law, University of Naples "Federico II"; legal chief of the public/private partnerships "FAIR" and "Restart", funded by the European Union.

[15] Aeschylus, Prometheus Bound (Italian translation edited by L. Medda), Milan, Mondadori, 1994.
[16] Aristotle, Nicomachean Ethics, VI, 3 (1139b–1140).

which, promoted to the role of "system architecture",[17] becomes the ordering criterion for the other sciences and, among them, also for technology, freeing human beings from subjection.

In the Aristotelian vision, technology serves politics because, as a means, it cannot do what lies within the availability of the end, namely politics. The means/end relationship should reserve for technology an inevitably ancillary position, a secondary role, ready to follow what comes before it. Politics, by contrast, must precede scientific knowledge and guide it towards the common good. [18] Between the two terms there is an inverse relationship: as one diminishes, the other expands.[19]

The main/accessory sequence respects the nature of politics as the art of quality and, at the same time, accommodates the opposite quantitative genesis of technology, resolving itself in recognising politics as having primacy over numerical magnitude. [20]

We shall try to understand whether this order of intervention between politics and technology has endured over time and, if the answer is negative, whether the thesis of technical neutrality is still sustainable: the idea of a masterless knowledge, without an owner, wandering without an objective to pursue. [21]

We shall examine how politics and technology have combined in a coexistence of variable proportions; [22] what lies behind this mixture; and on which step of the scale their precarious balance has settled. We shall reason about how to design a correct relationship between technology and law, capable of guaranteeing the basic principles of the democratic order: political responsibility, the rule of law and erga omnes protection of fundamental freedoms. Finally, we shall ask what role may still be reserved for the supranational political subject. [23]

---

[17]Id., Nicomachean Ethics, I, 2 (1094a–b).

[18]U. Galimberti, Psiche e techne. L'uomo nell'età della tecnica, Milan, Feltrinelli, 2021, 250.

[19]G. F. Pizzetti, "Decisione politica ed expertise tecnico", in G. De Minico – M. Villone (eds.), Stato di diritto. Emergenza e Tecnologia, Milan, Consulta OnLine, 2020.

[20]F. Salmoni, "Il difficile equilibrio del diritto costituzionale tra presunta neutralità della tecnica e scelte politiche", in Justiça do Direito, 2019, 33, 2, 152.

[21]S. Romano, "Mitologia giuridica", in Frammenti di un dizionario giuridico, Milan, Giuffrè, 1947, 126 ff., especially 134.

[22]N. Irti - E. Severino, Dialogo su diritto e tecnica, Bari, Laterza, 2001.

[23]U. Galimberti, Psiche e techne. L'uomo nell'età della tecnica, cit., 250–262.

8.2 Technology defines the uncertain elements of anticompetitive conduct

Technology intervenes on the rule that the antitrust legislator has intentionally left undefined, completing it so that the elastic provision can adapt without interruption to changes in the technical and economic situation while maintaining its wording unchanged.

Indeed, the provision gives little guidance on abuse, dominant position and the substantial alteration of competitive balance,[24] leaving it to the antitrust authority to define these elements case by case. The authority is entrusted with a preliminary yet essential operation for applying the rule to the concrete conduct under review: defining the undefined, completing what the lex mercatoria intentionally left unfinished.

How does the antitrust authority compose its filling parameter? Recourse to business disciplines is not enough because, being based on mechanistic causality, they reach debatable results lacking the necessary scientific objectivity; their highest degree of reliability lies in the professionalism of the interpreter. When the assessment of a fact is based on a technical parameter that is not securely established, the result is a "controversial scientific question",[25] due to unavoidable factors of uncertainty arising from gaps in scientific knowledge, to the point that, if the interpreter changes, opposite outcomes may be reached because decisions are affected by the mindset of the person who first defines the evaluative parameter.

Given the insufficiency of endogenous rules, the antitrust authority must choose what it means by competitive balance.[26] Three theses may help it, but the choice of one or the other will depend solely on its unreviewable will: the first favours consumer

[24]M. CLARICH, *Per uno studio* sui *poteri dell'Autorità garante della concorrenza e del mercato,* in F. BASSI-F. MERUSI, *Mercati e amministrazioni indipendenti,* Milan, Giuffrè, 1993, 123.

[25]L. Violini, Le questioni scientifiche controverse, Milan, Giuffrè, 1986, 136.

[26]M. Libertini, "Concorrenza" (entry), in Enc. Dir., Annali III, 2010, 191 ff.; R. Bork, The Antitrust Paradox: A Policy at War with Itself, NY, Basic Books, 1978; and R. A. Posner, Antitrust Law, Chicago, University of Chicago Press, 1976 (2nd ed. 2001).

protection over any other interest; the second protects existing competitors, that is, preservation of the status quo; the third looks ahead and guarantees the future elasticity of the market for competitors yet to come. Depending on the competitive model chosen, the authority will assess the conduct as unlawful and prohibit it, or as compliant with antitrust law and allow it.

Given this variability of judgment on the same conduct, how should the powers of the antitrust authority be defined? And how should the alternative be resolved between the paradigm of a quasi-judicial function and an unprecedented archetype of power?

The model of iuris dictio has a unidirectional outlook, realised by bringing a fact within an abstract statutory provision according to the equation "if A exists, B must follow"; this neglects the stage preceding that comparison: defining the parameter by which the conduct is to be judged. Whereas for the judge the already complete legal parameter is only to be interpreted, for the antitrust authority it is the beginning of a creative activity of law, because it must first fill the blanks left by the legislator with its volitional energy and its value choices. This reveals its aptitude for political action; it is no coincidence that the antitrust authority draws from the same toolbox as the political decision-maker: unlimited acquisition of data, circular information with top bodies and openness to dialogue with the base.[27]

Recognising that antitrust law already has an end constraint when it completes imperfect elements does not contradict the proposed comparison between the powers in question and the function of political direction, which, in constitutional interpretation, also exists where freedom as to objectives is limited, provided that the political prerogative specifies times, methods and articulations.[28]

The difference between the political decision-maker and the antitrust authority does not lie so much in the conflict between absolute and relative freedom of choice, but in the source from which the two draw the necessary suggestions for composing the identity of the end. Unlike the political decision-maker, who shapes the common good according to the political feeling of the majority of the day, the antitrust authority must

[27]M. Manetti, Poteri neutrali e Costituzione, Milan, Giuffrè, 1994, 197.

[28]M. Dogliani, Indirizzo politico. Riflessioni su regole e regolarità nel diritto costituzionale, Naples, Jovene, 1985, 201 ff.

not be guided by majority political will. Created to be unavailable to the command of the political elite, when closing the parameter of judgment it must not lean towards any of the forces in play: it must remain equidistant from hegemonic political families and from strong regulated parties. Here too, the comparison does not lead to a perfect coincidence between the ordering function of the antitrust authority and the political direction of the representative subject.

We may therefore say that we are faced with a hybrid figure of power: it shares with the judiciary the activity of judging conduct according to a legal parameter; at the same time, it is innovative in the way the antitrust authority completes the parameter of judgment, because it spends its volitional energies as a political decision-maker would when composing objectives and planning the means of future political action. A complete definition of these powers must combine the two moments: iuris latio in constructing the parameter and iuris dictio in applying it to the case under review. In short, it is a function assisted by a high degree of political character, mitigated by the brief and sparse statutory indications.[29]

Let us ask what effect this function, partly comparable to political direction, has on institutional balance.

Since legislative silence has shifted to independent authorities[30] the responsibility for mediating among the values at stake, merely listed but not developed in a dimension of reciprocal coexistence, the new authors of legality have been entrusted with the task of resolving the dispute over "desirable balances" in an original way, lacking incontrovertible evaluative parameters with which to compose the pacifying rule.

The general politics of elected representatives has progressively withdrawn to leave room for the sectoral politics of technicians who, although not always welcome to citizens, cannot be removed medio tempore because their office is not founded on a political mandate; this shields them from political responsibility for the decisions adopted.

[29]Reference is made to the reflections developed in: Antitrust e Consob. Obiettivi e Funzioni, Padua, Cedam, 1997, 277–280.

[30]Hereinafter "AI".

This intersubjective substitution has broken the political-representative circuit People–Parliament–Government, introducing a spurious element — the independent authority — that has placed popular sovereignty, the cornerstone of the republican edifice, under tension. Whatever the variability of its meanings, popular sovereignty remains indissolubly linked to the idea that the political-representative relationship is the only and irreplaceable channel of legitimation for political decision-making.[31]

Since it is correct to recognise the centrality of popular sovereignty as a limit to constitutional revision, not even recourse to Article 138 of the Constitution could bring the framework described so far back within constitutional legitimacy.

The issue is not whether independent authorities are compatible with the basic architecture; rather, the question is whether such a political prerogative, assigned to actors not even indirectly traceable to the popular will, is consistent with the institutional structure. Not even a constitutional revision rule could legitimately do this, because admitting it would bring about such a significant revisiting of the system's basic architecture as to exceed the limits of the power of revision, altering the identity traits of the democratic Republic.

Perhaps constitutional scholarship has not always grasped, and not always deeply enough, the implications of new modes of law production. As regards independent authorities, the issue has been reduced to whether they should be provided for in the Constitution;[32] but granting them constitutional visibility is not sufficient to justify the political prerogatives awarded to them.

Nor would a different conclusion follow from completing the conferral of the political function with a constitutional provision for adversarial participation with the regulated parties.

---

[31] E. Cheli, Atto politico e funzione di indirizzo politico, Milan, Giuffrè, 1961, 93.

[32] Two approaches emerged within the D'Alema Bicameral Commission: the minimalist approach, which sought to include as little as possible in the constitutional text, apart from the very existence of the Authorities themselves. In contrast stood the thesis advocating the full constitutional entrenchment of the Authorities' legal status, with the Authorities classified according to their fields of intervention and their respective powers. This latter method risked freezing a phenomenon which, instead, must remain flexible in light of the historical and political needs of the moment: A. ROUYÈRE, *Faut-il faire figurer les autorités administratives indépendantes dans la Constitution?*, in *Les petites affiches*, 1992, 56 et seq. See: M. MANETTI, *Autorità indipendenti: tre significati per una costituzionalizzazione*, in *Pol. dir.*, no. 4, 1997, 657 et seq.; S. STAMMATI, *Le autorità di garanzia e di vigilanza*, in S. PANUNZIO, ed., *I costituzionalisti e le riforme*, Milan, Giuffrè, 1998, 343 et seq.; and, if desired, G. DE MINICO, *Regole. Comando e Consenso*, Turin, Giappichelli, 2005, especially the Conclusions..

This is so for two reasons: the ontological diversity of political representation in terms of prerequisites, nature and effects as compared with representation of interests excludes the possibility of drawing from the former a legitimacy transferable to the latter, for the simple reason that such legitimacy is in the non-transferable availability of the former and not of the latter.

Moreover, if the People–Parliament–Government circuit is regarded as the only channel capable of transmitting the enabling title for political choice, it is an identifying feature of our legal order and, as such, admits no substitutes, even if designed by a constitutional revision rule. In short, the dialogue of independent authorities with the base cannot make up for the absence of substantive primary legislation.

In the conclusions we shall consider a possible way to overcome this institutional impasse, in which technology — having become authoritarian and absolute power — has displaced politics, which, deprived of its language of ends, appears to chase technology rather than orient it, ceding to it spaces of decision that, in a democratic order, should remain firmly in the hands of representative subjects.

8.3 Technology and digital markets

When the digital market began to establish itself, antitrust rules were not yet ready to include the anticompetitive conduct of e-economy entrepreneurs within the traditional categories of agreements and abuses. It is therefore necessary to recall the physiognomy of digital markets in order to understand the reasons for their initial exclusion from the traditional economy.

Technology first becomes an identifying feature of digital markets, absent from analogue marketplaces: these are double-sided markets dominated by gatekeepers (GK), neutral managers of the platform who are active not only in promoting the meeting of supply and demand but also in competing downstream with other competitors, who are forced to turn to them for use of the platform.[33] The GK is inevitably a vertically integrated operator, ready to repeat abusive conduct over time because of its physiological conflict of interest. Nor should one forget a natural effect of these markets: they can keep their customers tied to them (the so-called lock-in

[33] G. Pitruzzella, "Le libertà di informazione nell'era di Internet", in MediaLaws, 1, 2018, 23

effect). Although users may change platform, they will hardly do so because elsewhere they would not find better conditions. When Google provides us with a digital service in exchange for our data, it builds an accurate profile around us; thanks to that identikit, advertising will be tailored to each individual citizen-consumer, more targeted and therefore more likely to receive clicks; for this reason advertising spaces become more valuable and can be sold at a higher price than they would have without profiling.

Since technology has given anticompetitive wrongdoing a new curvature, how does it affect the interpretation of antitrust rules?

If technology is taken as an element integrating an evolutionary reading of the legal text, old antitrust rules, while their wording remains unchanged, would see the meaning of their provisions modified automatically and continuously as technology advances, also because of the elasticity of anticompetitive categories.

Moreover, this technically oriented interpretation would have the merit of not being deceived by appearances, because it would take conduct for what it is: repeatedly aggressive market behaviour, even when it does not show the classic and literal signs of abuse of dominance or prohibited agreement. A technique left to itself would be a dangerous "means to produce revenue and market control", [34] whose interpretative outcome would prevent rules from being porous to new offences. By contrast, a technique oriented towards the common good would not leave Big Tech undisturbed in appropriating citizens' data, protected by technological anarchy and by dominance that third parties cannot contest.

Here we observe changing attitudes on the part of the European Commission,[35] which may be summarised in three strands: a first, a second and perhaps also a third, in a forward-looking perspective.

A) The Commission initially considered that the conduct of Big Tech, even if harmful to privacy, fell outside its competence because it "fall[ed] out of the aim of antitrust law" [36]*,*

[34] S. Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, New York, Profile Books Ltd, 2019.

[35] Hereinafter referred to by the acronym: EC.

[36] M. Vestager, "Competition in a BD world", 18 January 2016, https://ec.europa.eu/commission/presscorner/detail/en/speech_16_5224.

since it was *"within the scope of the EC data protection rules".* This application of antitrust law, insensitive to the changed technological context, resulted in the use, as indicators of abuse and as criteria for identifying relevant markets, of the traditional quantitative parameters — based on payment for the transaction and substitutability of products — valid for analogue marketplaces but insufficient for digital ones. It would instead have been reasonable to adopt alternative criteria for assessing abuse: no longer the small but significant and non-transitory increase in price, incapable of shifting demand where digital transactions are free of charge, but the small but significant and non-transitory reduction in the quality of the service.[37] The new parameter is not free of uncertainties: how is a qualitative change in an immaterial value such as privacy to be calculated? And should the yardstick be the same for all subjects, or should it be measured according to customers' tendencies and their differing sensitivity to personal-data protection?

B) The second phase saw the Commission inclined towards more flexible attitudes because it realised that abuse could have symptomatic manifestations which were not even conceivable when Article 82 EC (now Article 102 TFEU) was drafted. Accepting technology as an element integrating an evolutionary hermeneutic — which I prefer to call a constitutional-by-design reading because of its ability to incorporate the principle of equality — meant admitting that technology had silently rewritten the antitrust offence, even though it had not done so explicitly: it had insinuated itself into the interstices, the spaces left unfinished by the Community legislature, bringing within prohibitions conduct that seriously compromises competitive balance and that would otherwise have remained hidden in the shadow of the rules, granting Big Tech permanent impunity.

b.1) Examples are provided by the recent 2024 Notice on relevant markets,[38] in which the Commission, for the purpose of identifying the relevant market, abandons the traditional product criterion in favour of a method modelled on the characteristics of

[37]M. E. Stucke - A. P. Grunes, Big Data and Competition Policy, Oxford, OUP, 2016, 115 ff.

[38]European Commission, Commission Notice on the definition of the relevant market for the purposes of Union competition law, C/2024/1645, https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX:52024XC01645, 30 ff.

digital marketplaces, where Big Tech supplies a bundle of multiple services. This persuaded the Commission to adopt a view of the market that is no longer atomistic but comprehensive, obeying the economic tendency towards the digital ecosystem.

b.2) As for the symptoms of abuse, in recent sanctions cases against Google or Apple one may observe that the Commission, having lost faith in the rigid separation of competences — according to which what belongs to the privacy authority is outside its concerns — adopted a very reasonable approach, respectful of the rule of assigning each actor its own role. Antitrust treats the privacy infringement as a vital clue[39], but does not consider it sufficient in itself to perfect the antitrust offence: it is only a warning bell, after which it must still be assessed whether market aggression exists. The Commission, like the Court of Justice (Grand Chamber, 4 July 2023, Meta Platforms Inc. v Bundeskartellamt), did not credit the suggestive thesis of the German antitrust authority, which had spoken of a "normative presumption", [40] committing the error of automatically completing models of harmful conduct. Had the Commission done so, it would have fallen into the opposite excess: from the absolute irrelevance of privacy to its absorption of every other assessment concerning competitive balance. Instead, it preferred an approach adherent to the facts, drawn both from aggressive market conduct and from the privacy infringement.

The Court of Justice (Grand Chamber)[41] observed that, when examining an abuse of dominant position, the antitrust authority may also ascertain the conformity of the undertaking's conduct with rules other than those falling within competition law, such as the provisions of the GDPR, [42] since their infringement represents an "important indication [...] for assessing the consequences of a given practice on the market or for

[39]Court of Justice (Grand Chamber), 4 July 2023, Meta Platforms Inc. and Others v Bundeskartellamt, ECLI:EU:C:2023:537; see also General Court, Sixth Chamber, extended composition, 14 September 2022, Google and Alphabet v Commission (Google Android), Case T-604/18, especially paragraphs 284–305.

[40]See Bundesgerichtshof (Federal Court of Justice), Decision KVR 69/19, 23 June 2020, and the related press release "The Federal Court of Justice provisionally confirms the allegation of abuse of a dominant market position by Facebook"; the Federal Court inferred a "normative causality" link from the conduct increasing the dominant undertaking's market power.

[41]European Commission / Court of Justice, 4 July 2023, Meta Platforms Inc. and Others v Bundeskartellamt, ECLI:EU:C:2023:537, especially paragraph 47.

[42]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=it.

consumers". Therefore, continuing to regard antitrust rules and privacy rules as independent sectors risks undermining the effectiveness of competition law if their separate interpretation becomes not episodic but recurrent.[43]

b.3) The third step, still to come, offers promising signs concerning the sanctioning system. Since pecuniary sanctions do not provide for an economic surplus beyond what is sufficient to compensate the harm caused, it is more convenient for the infringer to violate the rule than to comply with it, treating the sanction as an inevitable cost of its unstoppable expansion. The absence of a punitive element in the sanction has left Big Tech dominance unchanged; it has not slimmed down their unlawful acquisition of power or the repetition of abuses of dominant position, as shown by their continuous recurrence over time in almost identical ways.

Sanctions should instead make a qualitative leap, if only politics wished it, and turn towards measures restoring infringed rights, capable of bringing the law back to where it was before the infringement. If, however, the violation of rights is irreversible, the sanction must redefine the overall situation of the dominant undertaking and modify it radically, because that situation is precisely the cause of an offence that otherwise would not have occurred. The reference is to de-structuring sanctions (an example is Article 18 DMA), which break up the vertically integrated operator by ordering the loss of ownership of the platform so as to separate, from the previous ownership structure, its role as operator on the retail market; it is in that coincidence of status — neutral manager of access traffic and supplier of digital services in the downstream market — that the physiological conflict of interest to be eliminated is fulfilled.

At present, such sanctions have never been applied, apart from the timid beginning in the very recent Google AdTech 2025 case (AT40670)[44], where the Commission invited Google to submit a commitment proposal aimed at ownership separation of the data asset or, at least, isolation of part of the value chain in order to remedy at the outset this conflict of interest in re ipsa. These sanctions would promote, with a pro-future projection, the contestability of new markets in which there has been a wild transfer

[43] M. Vestager, Press release, Case AT.40684 - Facebook Marketplace, Brussels, 4 June 2021, https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2848.

[44] EC, *Press release*, in https://ec.europa.eu/commission/presscorner/detail/it/ip_25_1992.

and concentration of dominance, reducing protective barriers through data sharing or through the extreme measure of deconcentrating vertical integration.

C) This courageous antitrust revolution, only just begun, would require Big Tech to comply with the rules not as episodic fulfilment, an occasional event suggested by mere calculation of economic convenience — that is, only when it coincides with their individual interests — but as conscious conduct, dictated by the duty to respect the economic freedoms and fundamental rights of others, even when they do not align with their own selfish advantages.

In conclusion, the planes once separate — privacy and competition — are now mixed; goods once distant and exposed to distinct forms of conduct are now subject to progressive injuries or may be protected one as a consequence of the other; and authorities once unable to communicate are called upon to speak, because this intertwining of substantive law imposes an intertwining of powers and a productive "confusion" of procedures. In the face of an offence that causes a violation both of competition and of privacy, its return to legality must repair both attacked goods; otherwise one side of the offence would still remain without remedy.

Thus, a technically oriented interpretation of antitrust law, if kept away from typical legal assessments, shows undeniable advantages: it is pragmatic, obeys the principle of sincere cooperation between authorities (Article 4(3) TEU), is sensitive to privacy concerns, is well tailored to the dynamics of the digital economy, captures aggressive market conduct that would otherwise remain immune from punishment because of its technological novelty, and above all respects the centrality of the individual by granting rapid and efficient protection to infringed rights.

8.4 Technology from self-regulation to source of law

In the following reflections we shall outline the attributes of self-regulation[45], its legal regime and the requirements of constitutional compatibility when it is called upon to integrate the legal order at European level.

[45]Hereinafter referred to by the acronym: s.r.

Because of the variability of models, some scholars have described self-regulation as an umbrella concept;[46] nevertheless, it remains a form of the law of private actors,[47] because it consists of rules that the addressee has given to itself in advance, thereby eliminating the distance separating the regulator from the regulated.

The archetype, owing to Anglo-Saxon pragmatism and later adopted by the European legal order, marks a setback for top-down State law.[48] It breaks with the law as the exclusive source of the State's regulatory will and opens itself to law that initially arises without the State, since, as a set of negotiated rules, it did not need to ask the State for the imperativeness of legal norms, the limited inter partes effect of the regulatory agreement being sufficient. But the complexity of modern relations has demanded legal responses that are flexible, timely and close to moving reality; consequently, the legal order has left behind the monolithic and authoritarian model and moved closer to networked and bottom-up participatory forms. The State has begun to cede normative spaces to private collective subjects, which have proved capable of elaborating effective rules within their specific contexts of belonging.

Santi Romano's reflection provided the theoretical basis for the ongoing change: his concept of autonomy, understood not only as a faculty of the individual but as a structural datum of law, is the ideological premise of legal pluralism.[49] Every organised social group endowed with normative power and regulatory capacity may constitute a minor order ex se, to which the State recognises a space of action, not leaving it extra ordinem but integrating it within the systemic framework, provided it respects the conditions previously imposed on it. It should be made clear from the outset, however, that the State's openness to private sources has not meant a straightforward renunciation of its normative sovereignty; on the contrary, the State recognises self-regulation as an integrative form of the legal system on condition that it operates in

[46]The expression is due to L. Senden, Soft Law in European Community Law, Oxford-Portland, Oregon, Hart Publishing, 2004, 110.

[47]Reference is due to W. Cesarini Sforza, whose intuition produced the expression used in the text and the title of his work, Il diritto dei privati, Milan, Giuffrè, 1963.

[48]For systematic rigour, reference should be made to J. Black, "Constitutionalising Self-Regulation", in Modern Law Review, 59, 1996, 26.

[49]S. Romano, L'ordinamento giuridico (1st ed., 1918), 3rd ed., Florence, Sansoni, 1977, especially chapter II, passim; and Frammenti di un dizionario giuridico (entry "Autonomia"), Milan, Giuffrè, 1947, 29.

respect of constitutional principles and under its supervision. A model of co-regulation thus emerges, in which public authorities and private subjects share the normative function according to a precise division of roles and intervention times. The State becomes the "system architect", outlining institutional structures, defining general objectives and reserving the power of corrective intervention, while the law of private actors moves with some lightness within the terrain delimited by the State. In this context, private subjects entrusted with regulatory tasks must have a precise structural physiognomy guaranteeing adequate representativeness of base interests, transparency in decision-making processes, openness to discussion with external stakeholders and availability to public control.

This sharing of normative work between the legislator and private actors brings us back to our initial question: what is the relationship between politics and technology? Can we still say that technology is accessory to the primary norm if the latter has renounced a political language because it has resolved itself into setting the title of competence — the rule on legal production — while refraining from establishing specific objectives to be achieved and principles with which technology must comply? If this is so, that is, if a political perimeter is lacking, the code serves as both framework and frame: it begins the normative discourse and brings it to completion. The result is an inversion of the terms of the relationship: technology will speak in place of politics, with the aggravating factor that here the decision is made by private actors, not even by a public, pseudo-independent subject.

8.5 Conditions for the legitimacy of codes as sources

In this changed context, the concept of co-regulation is the plastic representation of the new system architecture: public and private actors cooperate in the process of constructing law, each according to its competences and its respective times of entry and exit from the political stage. In particular, the public promotes, orients and supervises; the private proposes, experiments and implements. [50]

[50] Thus R. Griffin, "Public and private power in social media governance: multistakeholderism, the rule of law and democratic accountability", in Transnational Legal Theory, 14, 1, 2023, 46–89.

The conditions of legitimacy for promoting self-regulation to a source producing objective law — that is, an act capable of generating abstract and general rules — are also the minimum requirements of its constitutional compatibility. For the reader's convenience, these conditions are divided into three distinct categories: subjective, procedural and teleological.

On the subjective level, the regulator must be a representative and democratically organised entity. Not every association can therefore assume normative tasks: legislative recognition is needed to identify ex ante the criteria of suitability, such as number of members, territorial diffusion and recognised public function. This is representativeness founded on objective criteria — membership, social relevance, historical continuity — assessed case by case and capable of guaranteeing the democratic nature of private decisions, which must be taken with the consent of the associational base and far from models imposed by a ruling elite.

From a procedural standpoint, the method for producing the rule is crucial: it must be inclusive, transparent and based on real, not merely formal, dialogue with the social parties, because only their effective involvement can guarantee a balanced normative process legitimised by its diffusiveness. [51]

Finally, the purpose of self-regulation must be adherence to the general interest, not narrow coincidence with the protection of dominant positions; hence the inadmissibility of rules elaborated for exclusive, predatory or discriminatory purposes. The regulatory procedure must therefore be "porous" — in the sense used by Teubner — to the participation of all regulated parties, including those with adversarial positions towards the private actors who first took the initiative, that is, the strong, well-structured and well-funded regulated parties, so that the rule is supported by a real in idem placitum consensus. This means that the elaboration of consensual rules is not the secret and exclusive reserve of dominant negotiating parties; rather, it must take place in the light of day and unfold through an equal and as widespread as possible dialogue among every category of subjects regulated by the negotiated rule. Private

[51] The author's work "A Hard Look at Self-Regulation in the UK", in European Business Law Review, 2006, 17, 1, sets out methodological observations for bringing the structure of private regulatory authorities within constitutional compatibility.

law shared in its making will be less odious to those who must observe it, because they have contributed to creating it. [52]

A different question is whether a genesis balancedly agreed between the opposing parties to the normative agreement can make up for the lack of political legitimacy of the private regulator. We believe that, even if participatory diffusiveness could compensate for the initial asymmetry between contracting parties, at most it would create a complete representation of interests, which nevertheless remains a distinct entity and cannot be superimposed on political representation, because of the autonomy of the respective interests defended and aims pursued. The former displays only individual values; the latter, by contrast, is projected towards the common good, which is not the atomistic parade of individual subjective positions but their reading, first analytical and then synthetic, from the perspective of the public interest. The irreducibility of one entity to the other excludes any reciprocal substitution, because what is available to one type of representation is not available to the other. [53]

The legal impossibility of private representation operating in place of political representation allows us to resolve the thorny issue repeatedly addressed in European law, which has tried to clarify the breadth of the decisum legitimately entrusted to private actors. The question, initially concerning delegation to committees — public subjects ancillary to the Commission — may be extended by analogy to delegation of the European legislative function to private actors. In this case too, the conditions of legitimacy laid down in Meroni[54] apply: they tended to exclude delegation of purely political regulatory tasks, or of tasks characterised by a high degree of discretion or involving antithetical value choices. Were this the case, we would be faced not with the exercise of a function under the control of the delegating authority, but with its transfer, with the inevitable attribution of political responsibility to the transferee and an

[52]W. Streeck - P. C. Schmitter (eds.), Private Interest Government, London, Sage Publications, 1985; S. R. Ackerman, "Consensus versus incentives: a skeptical look at regulatory negotiation", in Duke Law Journal, vol. 43, 1206, 1994, 1216–1217; and, in Italian scholarship, C. M. Bianca and P. Rescigno on private authorities and internal justice in associations.

[53]On this point, reference is made to the author's study Regole. Comando e consenso, cit., especially chapter II.

[54]Court of Justice, Meroni v High Authority, Case 9/56, 13 June 1958 [1957–1958], ECR 133.

alteration of the original architecture of the Treaties: "The intent is clear. Policy choices remain for the Commission; implementation is for the Agency".[55]

This substantive limit on delegation[56] contributes to defending the institutional balance, which not even its most dynamic[57] interpretation has managed to expand without compromising the spheres of competence defined in the Treaties. This limit requires each institution to "exercise its power with due regard for the power of other institutions", and entails that "it should be possible to penalize any breach of that rule which may occur". In short, the principle recalled does not allow definitive and unilateral shifts of decision-making powers which, by involving political assessments by subjects outside the original institutions, would inevitably bring external shifts of responsibility, if not the creation of areas immune from political control.

In the interpretation of the supreme judge, which favoured a dynamic conception of self-regulation over a more formal one that would have kept it outside judicial review,[58] the principle in question represents the thin boundary line separating the political decision, reserved to the European legislator called upon to speak first, from the act of self-regulation, which must instead follow, develop and articulate the political discourse already begun by its predecessor. Respect for the principles of common European constitutionalism — equality, freedom, responsibility, in a word the democratic nature of the system — is therefore the necessary condition for the legitimacy of delegating normative powers to private actors. Only respect for the three planes into which the sharing of the normative task with private actors is articulated — subjective, procedural and teleological — allows the European institutions to recognise self-regulation as a source within the legal system. In the absence of these

[55]P. Craig, "The Constitutionalization of Community Administration", in European Law Review, 28, 6, 2003, 849.

[56]Court of Justice (Grand Chamber), 22 January 2014, C-270/12, https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX:62012CJ0270.

[57]E. Chiti, "Beyond «Meroni» the community legitimacy of the provisions establishing the European agencies", in G. Cananea (ed.), European Regulatory Agencies, Paris, ISUPE Press, 2004, 83.

[58]A. Poggi, "Soft law nell'ordinamento comunitario", 2005, https://www.associazionedeicostituzionalisti.it/old_sites/sito_AIC_2003-2010/materiali/convegni/aic200510/poggi.html, para. 3.

safeguards, the private rule must remain a contractual act whose effect is necessarily limited to the private parties alone.[59]

8.6 Do the codes provided for in the DSA comply with the model of constitutional compatibility?

The Code of Conduct on Disinformation, provided for by Article 45 DSA, is a clear example of a co-regulatory process because the proposal of the private side, subjectively complex, was shared by the Commission, which repeatedly indicated substantive and procedural adjustments to the private draft. Thus the initial 2018 draft, criticised with observations specific comments by the Commission,[60] was followed by the latest version,[61] now integrated into the DSA[62] and the subject of an Opinion that is broadly approving by Brussels. [63]

In line with the theoretical approach indicated above, we shall verify whether the act possesses the subjective and objective requirements of legitimacy necessary for its inclusion among the sources of law.

There are two conditions for the institutional compatibility of this division of labour between the European legislator and private regulators: the former must (a) design the internal physiognomy of these private interest governments and (b) reserve to itself the political direction of the developments of self-regulation, orienting private power no differently from how it would do in the delegated exercise of the normative function;

[59]This is the Code of Practice on Disinformation of September 2018: a self-regulatory code containing 21 commitments in several areas, from transparency in political advertising to demonetisation of disinformation promoters. See https://digital-strategy.ec.europa.eu/it/library/2018-code-practice-disinformation.

[60] Si tratta del *Code of Practice on Disinformation* del settembre 2018: un codice di autoregolamentazione contenente 21 impegni in diversi settori, dalla trasparenza nella pubblicità politica alla demonetizzazione dei promotori della disinformazione. In *https://digital-strategy.ec.europa.eu/it/library/2018-code-practice-disinformation*.

[61]The Code of Conduct on Disinformation, published in June 2022, was republished on 13 February 2025 following integration into the DSA, with an updated Preamble. The most recent version is available at https://disinfocode.eu/the-code/read; the website is also the Transparency Centre under Chapter VIII of the Code.

[62]Under Article 45(4) DSA, the integration of Codes of Conduct is subject to the double positive opinion of the European Commission and the European Board for Digital Services.

[63]European Commission, Commission Opinion of 13.2.2025 on the assessment of the Code of Practice on Disinformation within the meaning of Article 45 of Regulation 2022/2065, https://digital-strategy.ec.europa.eu/en/library/code-conduct-disinformation.

while the private actor is responsible for development and implementation within the framework outlined by the former.

As regards the subjective profile, private authorities should display a democratic identity and an internally articulated board capable of representing the full range of antagonistic interests involved in the matter to be regulated, because they are field assistants of the public subject, as the US Supreme Court reminds us: "Lindke sued Freed under 42 U. S. C. §1983, alleging that Freed had violated his First Amendment rights. As Lindke saw it, he had the right to comment on Freed's Facebook page, which he characterized as a public forum. Freed, Lindke claimed, had engaged in impermissible viewpoint discrimination by deleting unfavorable comments and blocking the people who made them". [64]

By contrast, the DSA codes are dictated by private actors whose identity is compressed onto only one side of the relationship, the industrial side, with the substantial omission of the weaker side, which will nevertheless be subject to rules imposed by the well funded and well structured counterpart that it did not choose. Here, law of spontaneous genesis, droit doux as the French say, is more imperative than heteronomy, because it is based on presumed consent which, even if given by weak private actors, has not gone through a procedural experience or even external visibility. Indeed, we do not know whether and what participants other than Big Tech observed on the draft presented to them already complete in every part; whereas, for an effective equality of all interested parties at the negotiating table, it would have been preferable for Big Tech to follow a negotiating model beginning with a notice and comment scheme, namely a list of open-ended questions left to the decision-making discretion of the contracting parties, rather than a unilaterally composed text articulated in regulatory boxes already fully filled in content.

As for disclosure, this attribute was entirely absent during the negotiation phase, so we do not know whether any comments from weaker parties were accepted and to what extent. In short, the contract was not valued as a moment for rebalancing an initial negotiating asymmetry between misaligned parties; consequently, assigning the label

[64]US Supreme Court, 15 March 2024, Lindke v. Freed LLC, 2024, 601 U.S. 187.

of contracting parties also to subjects other than Big Tech means being satisfied with the merely formal fact of their signature at the foot of the act. In terms of content, however, the rules for weaker contracting parties will be more commanded than those imposed by heteronomy: in short, we are faced with a law that is apparently consensual but, in substance, unilateral and imperative.[65]

As to the aims, these should be predefined with such precision as to ensure that politics chooses the type of risk, its extent and the method of assessment; among these three options, the main one is identifying the step of the ladder of risk at which acceptable danger is to stop. Deciding how much injustice is allowed, and from what point injustice becomes intolerable, is in fact a political issue because it concerns a precise qualitative and quantitative idea of justice and equality to be realised.[66]

To these critical reflections, which refer to a political decision handed blank to private actors, one should nevertheless add a note of appreciation for the difficult negotiation between Big Tech and the Commission, which produced an act aligned with the objectives of the DSA — indicated in sections II–VII of the 2022 Code — responsive in the measures for achieving those objectives and precise, in response to the Commission's remarks, as regards the indicators for detecting, qualitatively and quantitatively, the degree of fulfilment of the promised objectives.[67]

Consider, for example, measure 21.1, which requires the placing of labels indicating fact-checkers' assessments; notices to users who attempt to share, or have previously shared, the assessed content; and the immediate visibility of information panels on content reported by fact-checkers as violating their policies.

The main question for a constitutional lawyer nevertheless remains open: is this model of co-regulation consistent with the political-representative circuit or not?

---

[65]The Preamble to the Code states that the signatories themselves are its authors: "It is in this spirit that the Signatories have drafted the present Code identifying the commitment areas and measures each Signatory is making", Code of Conduct, 5. The Commission Opinion is more explicit, stating that "the Commitments, Measures and KPIs of the Code of Practice on Disinformation were negotiated between a very diverse community of stakeholders", cit., 14.

[66]Each commitment is structured into specific measures that signatories must implement according to the nature of their services; for almost every measure, QREs (Qualitative Reporting Elements) and SLIs (Service Level Indicators) are also indicated to measure the effectiveness of the measures. The signatories also undertake to develop, within nine months of signature, Structural Indicators (Commitment 41) to understand the overall impact of the Code.

[67]Code of Conduct, 28.

This is a breach which, unlike the one initially caused by the substantially primary regulation of independent authorities, will be more difficult to repair in the case of co-regulation, because the derogation is more subtle than the previous one: the private authority presents itself as a harmless self-regulator, only to betray its private origin when its rules, exceeding inter partes effect, bind a subjective sphere broader than the associational base that self-regulates.

This model is not without consequences for the institutional structure because, given asymmetric bargaining in favour of the strong, co-regulation violates the principle of formal equality: the substantially omitted private party will suffer an invasion of its sphere of autonomy which, in the absence of private power strengthened by public binding force, it could have rejected; conversely, private authorities invade another's individual sphere, an action they could not undertake without this ex lege authorisation.

If we transfer this reflection to the terrain of sources and then to the legal order, for technique to be a cooperative element of the system it must be able to exhibit the European norm not as a mere enabling title to create objective law, but as a principle of substantive discipline already immediately shaping the relationship, whose future developments are entrusted to harmonising technique.

It follows that the source which should be placed one step below European law does not, in concrete terms, speak second, because politics did not initially lay down an essential language; this inversion in the order of interventions along the regulatory chain means that the code assumes responsibility for the first move as well as for its subsequent developments.

Here, the realisation of the common good becomes a future and entirely uncertain event, depending on its occasional coincidence with the selfish interests of private interest government, in the absence of a serious framework ensuring that co-regulation obeys its social vocation.

Economically structured private actors, improper possessors of our data, who should be docile executors of a public task and available to the mise en place et de la mise en oeuvre des politiques publiques, are yet another myth created by the illusion of a technique at the service of human beings; for the moment, however, the DSA has

introduced private authorities that are aggressive and little inclined to realise human centrality.

8.7 The Artificial Intelligence Act and its claim to orient technology towards the human person

Let us examine the Artificial Intelligence Act[68] from the perspective of its promise: to bend AI towards the centrality of the individual. A few remarks are needed on the type of regulatory model introduced in the digital market, followed by an assessment of whether or not its ambitious promise is kept.

Let us begin briefly, for the purposes of this discussion, by saying what artificial intelligence[69] is. Its identity coincides with a learning process, guided by the human mind but also capable of autonomous evolution; [70] it feeds on growing masses of data,[71] with which it produces, on the basis of automatic assessments, the serial content of public or private decisions.

The way AI proceeds unfolds along two axes. The first concerns the method of its reasoning: statistical-correlational in nature, it prospectively anticipates the occurrence of probable situations on the basis of *id quod plerumque accidit*[72]. The second axis concerns the effects of intelligent action: these tend at least to orient, if not also to shape, the conduct of broad communities of people.

The logical path of AI has its focus in an ex ante prognosis. This forecast concerns the initial moment, in which Intelligence anticipates a probable future event — for example, a criminal act — but also the final moment, in which the mechanical mind outlines a policy of conduct, increasing in its obligations as risk increases, because it is

[68]Regulation (EU) 2024/1689, cited above, hereinafter referred to as the AI Act. For Italian and foreign doctrinal references, see the author's essay Giustizia e intelligenza artificiale: un equilibrio mutevole, in Riv. AIC, 2/2024, 86 ff.

[69]Hereinafter referred to by the acronym: AI.

[70]Thus U. Ruffolo - A. Amidei, La regolazione ex ante dell'intelligenza artificiale tra gestione del rischio by design, strumenti di certificazione preventiva e "autodisciplina" di settore, in A. Pajno - F. Donati - A. Perrucci (eds.), Intelligenza artificiale e diritto: una rivoluzione?, Bologna, Il Mulino, 2022, I, 493.

[71]Reference is made to the author's work Big Data e la debole resistenza delle categorie giuridiche, in Dir. Pubbl., 1, 2019, 90.

[72]V. Mayer-Schönberger - K. Cukier, Big Data. Una rivoluzione che trasformerà il nostro modo di vivere – e già minaccia la nostra libertà, Italian translation edited by R. Merlini, Milan, Garzanti, 2013, 16.

directed at preventing future and uncertain danger from degenerating into concrete and current harm to the fundamental freedoms of third parties.

Since AI risk is the ineliminable factor of the regulation under examination, the latter follows a precautionary model, where the adjective underlines its capacity to anticipate a harmful event and try to avoid it by imposing precautionary rules of conduct on operators. If observed, these rules generate in the community a relative certainty as to the safety of the machine and create legitimate trust that things are going in the right direction, namely that no harm will occur. The rules will tell the operator, in legally binding or soft-law language, how to choose the compositional elements of AI, how to train datasets, how to ensure their conservation, fairness and non-discrimination, how to assess inputs, how to carve out a space for human intervention and, finally, how to articulate the logic leading to the output. The precautionary discipline does not end with designing the abstract paradigm of an artificial brain, because once placed on the market it will continue to be accompanied by precise rules requiring the provider to update it, monitor it and, where necessary, correct it, including through the extreme measure of withdrawal from the market in cases of irreversible harm.

The fact that the AI Act followed a risk-based approach gave its regulatory technique a particular inclination: it consists of typical legal assessments that categorised activities into three types according to the level of risk. Some are absolutely prohibited because of the unacceptability of the potential danger; others are high-risk, admitted because the check and balance between innovation and fundamental freedoms allows them, subject to precautionary rules minimising risk; [73] finally, others are characterised by such slight risk that they are exempted from the most burdensome rules, as required by proportionality between the level of risk and the regulatory burden.

The reasoning is based on the assumption that compliance with abstract legality will isolate fundamental rights from the danger of injury, creating an appearance of lawfulness, that is, a guarantee for the community that everything will go well. If this should not happen and rights are infringed, the rules on liability for damage will apply; however, they are still looking for an author in the European legal order after the

[73] S. Heiss, Artificial Intelligence Meets European Union Law: The EU Proposals of April 2021 and October 2020, in EuCML, 6, 2021.

withdrawal of the proposal for a directive on liability for damage caused by artificial intelligence,[74] which also leaves the injured party's claim for compensation unsatisfied, assuming that injury to fundamental rights can be compensated with money.

This, then, is the substantive core of the precautionary discipline, but its effectiveness will depend on how compliance with the rules is ensured. Therefore, the formal profile too should be oriented towards the precautionary objective, if preventive regulation is to succeed. Here, the AI Act has reproduced the classical models of the control function:[75] prior review of automated activities not yet launched, and subsequent review of those already under way.

Prior control, appreciable as an idea, is disappointing in its implementation because the legislator did not require the provider to submit the system to an external and public certifier, being satisfied with a simple self-declaration — so-called self-compliance — attesting compliance with the prudential discipline. The subjective coincidence between controlled and controller, that is, this physiological conflict of interest, compromises the objectivity of the review, which is structurally unsuitable to offer the guarantees of neutrality necessary to reassure third parties, even though the AI Act does know the model of prior external control, which it uses only in residual and exhaustive situations (Article 43(1), second subparagraph), because it is excessively burdensome for the private actor.

During the preparatory work on the AI Act, many criticisms were directed at self-compliance because of the weak objectivity of self-assessments and audits in place of impartial checks by third-party reviewers. A robust audit not only guarantees citizens' rights but also facilitates downstream users, namely those who will build further systems on AIs already present on the market. [76]

What has been said makes self-compliance and the other self-declarations scattered through the text the real weak point of this discipline, which, in the name of decision-

[74]European Commission, Withdrawal of the proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence, C/2025/5423, 6 October 2025, https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=OJ:C_202505423.

[75]G. Ferrari, Gli organi ausiliari, Milan, Giuffrè, 1956, 270 ff.

[76]C. Dunlop, Policy Briefing. An EU AI Act that works for people and society. Five areas of focus for the trilogues, 6 September 2023, https://www.adalovelaceinstitute.org/policy-briefing/eu-ai-act-trilogues/.

making speed, has replaced authoritative controls with declarations of good conduct by the directly interested party, which should instead have been subjected to careful verification by an impartial public subject.

Finally, one last act of the prudential discipline borrows the form of self-declaration: the "fundamental rights impact assessment".[77] This is an anticipated judgment on the risks that Intelligence could pose to rights and is entrusted by the AI Act to the AI provider itself; but this intentional subjective coincidence nullifies the protective function of the assessment, because its internal author, less scrupulous than a third party in representing things, may present as minimal risks that are not minimal and weaken mitigation measures. It was expected to be an incisive instrument if the wording adopted in the European Parliament's amendments had been respected;[78] instead, it was seriously weakened in the text approved by the trilogue,[79] both because it was made mandatory only for certain providers[80] and because the deployer assesses impact only on subjects, not also on fundamental rights, unlike what the Parliament's amendments had provided.

With these variations on self-assessment, the public-law system continues its unstoppable race towards private-law involution, as shown by two circumstances: many situations remain outside the impact assessment, and its performance, closed to third parties, does not even contemplate public input, because it does not inform the national authority in advance; the latter can intervene only after the event. Late public intervention is an oxymoron for a discipline that aims to be precautionary and to improve the enjoyment of rights, not to compromise them, a result that self-risk-assessment certainly cannot guarantee.

[77]Fundamental Rights Impact Assessment, FRIA, under Article 27 AI Act.

[78]European Parliament, Compromise Amendments (COM(2021)0206 – C9 0146/2021 – 2021/0106(COD)), 9 May 2023, Article 29a (now Article 27).

[79]Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts - Analysis of the final compromise text with a view to agreement, 26 January 2024, Article 29a (now Article 27).

[80]More precisely, Article 27 limited it to public and private providers of public services, and to providers of social scoring or risk insurance.

Thus, the promise of human-centric AI is still waiting to be fulfilled because, at present, it is unbalanced in favour of well-funded and well-structured private actors. In this situation it is difficult to believe that the European legislator really intended to strengthen citizens' trust in the automated process, since it did not create the conditions for this to happen.[81] Indeed, the system reveals a basic contradiction: in the recitals the political decision-maker promises the centrality of the person and human dominion over the machine; in the operative provisions it forgets the promise made a few lines earlier.

Appreciating a risk-based regulatory approach does not conceal the defects of an AI system resting on a chain of uncontrolled presumptions, written under the dictation of lobbies[82] and heedless of possible prejudice to fundamental rights. Moreover, these mechanisms, unsupported by solid public control, risk deceiving citizens with empty legal certainties,[83] with fictions of legality that generate unjustified reliance on situations apparently lawful but substantively unlawful, just like that "Christmas tree and pretty lights" mentioned by Feigenson,[84] whose lights even the most hostile judge cannot resist.

8.8 Technology as a "source of law"

Technology takes a further step forward, moving from an element integrating the norm or its provision by will of the law to a source of law by self-promotion. In this action, technology radically alters the traditional paradigm of private law because it designs

[81] M. Draghi, Speech at the European Commission conference "One year after the Draghi report: what has been achieved, what has changed", Brussels, 16 September 2025, https://www.eunews.it/2025/09/16/un-anno-dopo-il-rapporto-draghi/, with reasoned criticisms of the European design on AI: excessive rules prevent AI from acting as a driver of competitiveness, reducing it to an obstacle to innovation.

[82] P. Friedl - G. G. Gasiola, Examining the EU's Artificial Intelligence Act, in VerfBlog, 2024/2/07; Corporate Europe Observatory, Byte by byte: How Big Tech undermined the AI Act, 17.11.2023, https://corporateeurope.org/en/2023/11/byte-byte.

[83] The expected Digital Omnibus (COM(2025) 837 final), in the European Commission's Digital Omnibus Package, still under way, in its attempt to simplify rules and procedures, does not appear to grasp the defects illustrated above, because it lightens the rules for large operators and, on the other hand, deprives citizens of effective precautionary protection.

[84] N. Feigenson, Brain imaging and courtroom evidence: on the admissibility and persuasiveness of fMRI, in International Journal of Law in Context, 2, 3, 2006, 246.

rules of conduct without resorting to human mediation; in this absence of the individual it breaks with the classical system of sources.

Indeed, its peculiarity lies in being a self-sufficient source, which begins and concludes the regulatory process alone: the circle begins and ends in technology. In short, everything is resolved in the statement of the artificial mind. This situation occurs when — to offer one of many examples — the DSA[85] and the platforms' self-regulatory codes[86] do not define the category of false or defamatory news.[87] Therefore, in order to know the prohibition in advance, it becomes necessary to read the concrete acts of cleaning carried out by online platforms.[88] Thus the normative chain descends to the lowest level of the codes and coincides with the concrete measure aimed at removing false, denigrating or violent news.[89] As a result, abstractness and generality are converted into the concreteness and particularity of the mechanical removal measure, to the detriment of certainty and equality of law.

---

[85]Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a single market for digital services and amending Directive 2000/31/EC, https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32022R2065.

[86]In Anglo-Saxon legal scholarship, mention should be made of the innovative thought of A. OGUS, *Rethinking self-regulation*, in *Oxford Journal of Legal Studies*, 15, 1, 1995, 99–100, who, rather than relying on predefined labels, preferred to study self-regulation according to the degree of decision-making autonomy, legal force and monopolistic power enjoyed by the self-regulating body: "to appreciate the range of possibilities [...] which can properly be described as 'self-regulation'". J. BLACK, *Constitutionalising self-regulation*, in *Mod. L. Rev.*, 59, 1996, 26, instead emphasized the need for a shaping intervention by the State where the rules adopted by the collective body are not exclusively "tailored to the circumstances of particular firms", but are imposed on the entire relevant social category. For further developments in Anglo-Saxon literature, reference may be made to our work: *A Hard Look at Self-Regulation in the UK*, cit., 183–211.

For a broad treatment of the formal and substantive aspects of platform self-regulatory codes, see at least: A. SIMONCINI, *La co-regolazione delle piattaforme digitali*, in *Riv. Tri. Dir. Pubbl.*, 4, 2022, 1031–1049; G. DI COSIMO, *La co-regolazione delle tecnologie digitali: il paradigma centro-periferia*, in *Oss. sulle Fonti*, 1, 2024, 272 et seq.; O. POLLICINO, *Regolazione e innovazione tecnologica nell' "ordinamento della rete"*, in *Riv. AIC*, 2, 2025, 169; L. TORCHIA, *I poteri di vigilanza, controllo e sanzionatori nella regolazione europea della trasformazione digitale*, in *Riv. Tri. Dir. Pubbl.*, 4, 2022.

[87]For a broad examination of platforms' behavioural obligations, see M. Orofino, Il Digital Service Act tra continuità (solo apparente) ed innovazione, in F. Pizzetti (ed.), La regolazione europea della società digitale, Turin, Giappichelli, 2024, 144.

[88]A. Lamberti, La libertà di manifestazione del pensiero "in trasformazione", in Riv. AIC, 3, 2025, 340.

[89]A. Lucarelli, Nuovi mezzi di comunicazione, assetti imprenditoriali e soggettività politiche, in Riv. AIC, 3, 2025, 103.

The DSA has therefore assigned gatekeepers a new public function: cleaning the network of false news. This is a task that a democratic order should not assign even to a public subject, because it presupposes the prior design of a paradigm of truth. The European act goes beyond this limit: it not only delegates the cleaning function to the private actor, but also exempts it from observing the formal and substantive guarantees necessary to delimit power when it encounters fundamental freedoms. Here both the guarantee of the rule of law fails, because there is no ex ante definition of the concept of falsehood, and the guarantee of due process fails, because content control takes place inaudita altera parte for reasons of speed. [90]

Moreover, the absence of an abstract and general definition of the concept of falsehood leaves gatekeepers free to confuse falsehood with news that is politically inconvenient or not aligned with dominant thought.[91] This regulatory vacuum in the DSA leads to tautological reasoning according to which hateful or violent conduct is prohibited because it is prohibited. This vicious circle may hide dangerous freedom-restricting theses and easy slides towards a single lawful discourse: the discourse of the State. This risk is inevitable in the absence of a legal parameter defining the concept of falsehood in advance, with the paradoxical result of a sharp divide between the offline environment, where dissemination of false ideas is not a crime unless it attacks interests other than truth, and the virtual environment, where the allegedly false idea moves from the exercise of a right to an unlawful act.

This way of proceeding eliminates legal certainty, the citizen's claim to advance knowledge of the rule, and covers everything with a veil under which lawful and unlawful, permission and prohibition, mix until they become indistinguishable from one another without any break in continuity.

To the political control of private actors over the ideas of other private actors we prefer the beneficial virtues of the marketplace of ideas, which, by allowing falsehood to

[90] I. Buri - J. Van Hoboken, The Digital Services Act (DSA) proposal: a critical overview; J. Laux - S. Wachter - B. Mittelstadt, Platform Regulation, Independent Audits, and the Risk of Capture Created by the DMA and DSA, in Computer Law & Security Review, 43, 2021; M. L. Chiarella, Digital Markets Act (DMA) and Digital Services Act (DSA): New Rules for the EU Digital, in Athens Journal of Law, 9, 1, January 2023; M. D. Cole - C. Etteldorf - C. Ullrich, Updating the Rules for Online Content Dissemination, Baden-Baden, Nomos, 2021.

[91] Arguing in favour of private censorship: C. Pinelli, Disinformazione, comunità virtuali e democrazia: un inquadramento costituzionale, in Dir. Pubbl., 1, 2022, 180 ff.

coexist with truth, leaves citizens the task of distinguishing between them because they have sufficient maturity to form their own view, without being pre-directed by those who claim to know for them what truth is. "In other words, the government's control over speech as an intellectual arbiter of the truth must be constricted, if not completely denied. Baked into the architecture of the First Amendment then - at least from a structural rights interpretation - is a deep skepticism about the good faith of those controlling the government. That skepticism flows from two facts: (1) decisions about what is true or false, when made by those in power, are bound up with political perspectives that the government seeks to undermine; and (2) the government's natural tendency [is] to twist reality to its own purposes". [92]

The replacement of the human mind by the artificial mind generates a complete, particular, ad personam "technical rule", attributable to synthetic will, before which the human in the loop is reduced to a merely verbal claim of the centrality of the individual; while the right to interact with a flesh-and-blood person, although recognised by law, has left no trace of itself in the creative process of the rules: yet another myth added to the many others created by the AI Act.

Let us now reflect on what it means to exclude the person-subject from the normative process.

When technology becomes source of law, a "subject-non-subject" enters the political scene: AI authorised to speak the law in place of human reason. The human attribution of the source-act thus collapses, because we are faced with a fact not traceable to a volitional moment of the individual: what is missing here is the intentional energy of the person, which in the source-act occupies the deliberative segment of the normative decision. [93]

To affirm a volitional void does not mean reducing AI to an entity incapable of knowing and reflecting; this is shown by the fact that the AI Act asks Intelligence for a result, whose fulfilment requires awareness and argumentative logic: writing a reasonable statement of reasons in support of the intelligent decision. This reasoning presupposes

[92] C. Calvert - S. McNeff - A. Vining - S. Zarate, Fake News and the First Amendment: Reconciling a Disconnect Between Theory and Doctrine, in U. Cin. L. Rev., 2018, 86, 99, 134.

[93] A. Cardone, "Decisione algoritmica" vs Decisione politica?, Naples, ES, 2021, 159.

that AI is able to make deductions according to causal criteria, no differently from the human mind. If this comparison of reasoning between the two intelligences is supported in philosophy,[94] we are not ready to adhere to either of the theses in play because they are scientifically immature; but we can observe that the reasoning underlying the statement of reasons is still a deficient aspect of the algorithmic act, lending itself to easy challenges for inconsistency of the reasoning with the abstract model laid down by the European legislator. Therefore, if the statement of reasons is the only element that brings AI closer to human intelligence, it proves little, since AI fulfils the duty to give reasons in an unsatisfactory measure.

But even if we admit that AI has dianoetic capacities, [95] this recognition does not cure its inability to train itself in ethical virtues, which are essential for making value choices in order to design a desirable balance between opposing interests, as the human legislator does.

AI cannot construct its own value heritage by itself; [96] therefore it will be for the human mind to educate it in ethical language and direct it towards that combination of goods designed by politics, which, as Aristotle wished, has the fundamental task of correcting the autonomistic tensions and selfish falls of a technique left to itself.[97] Here our argument connects with the initial reflections.

In the case of technique-as-source, however, it is both the beginning and the end of the political decision, which is entirely resolved in the artificial determination, enabled to write on an almost blank slate. This model of technique tolerates no limits because, strong in its self-legitimation, it recognises no authority above itself. For this reason it goes where it wants, heedless of any political responsibility, from which it is relieved because, to be responsible, someone must invest another with a political mandate, for

[94]S. Bubeck, V. Chandrasekaran, R. Eldan et al., Sparks of Artificial General Intelligence: Early experiments with GPT-4; R. Kurzweil, The Singularity is Near: When Humans Transcend Biology, London, Penguin Putnam Inc., 2006; D. Dennett, From Bacteria to Bach and Back: The Evolution of Minds, NY, W. W. Norton & Company, 2017; for an alternative view, J. R. Searle, Minds, Brains, and Programs, in Behavioral and Brain Sciences, 3, 3, 1980, 417–457.

[95]Reference is made to the opening paragraph on the Aristotelian definition and the antagonism between ethical and dianoetic virtues.

[96]For a contrary view: E. Severino, in N. Irti - E. Severino, Dialogo su diritto e tecnica, cit., 52.

[97]L. B. Solum, Artificially Intelligent Law, in BioLaw Journal, 1, 2019, 57; also A. D'Aloia, Intelligenza artificiale, società algoritmica, dimensione giuridica. Lavori in corso, in Quad. Cost., 3, 2022, 667–670.

which the latter must account to the former as mandator. In short, autogenesis gives it the privilege of absolute impunity.

Nor could the search for a politically responsible subject for the choices made be compensated by the accountability of the machine. This idea creates more problems than it seeks to solve, including the temporal irremovability of technique, which could endure indefinitely, escaping the risk of being replaced, as instead happens with an elected representative no longer appreciated by voters, who are free not to renew the initial trust for a subsequent mandate.

Nor could the lack of responsibility be recovered through a by-design technique, because anticipation of the threshold of unlawfulness, by inserting into the mechanical blender the essential elements for adapting it to the parameter of legitimacy, works fairly well when harm must be avoided, that is, when precautionary measures are designed to prevent the harmful event. If, however, the centre of the issue is the judgment of political responsibility, since this is an assessment of conduct whose effects have already occurred, it cannot be anticipated by a technique oriented towards including popular participation in place of political-representative participation. This substitution is not only incorrect because it places on the same level entities that cannot be aligned — as already explained with regard to independent authorities and private authorities — but here it also commits an error of timing: the time of judgment must necessarily follow the time of conduct. Therefore, if the substitute measure is laid down in advance, it cannot function as compensation for the absence of responsibility, because one cannot judge what has not yet happened; the democratic wound caused by the flight from accountability thus remains open.[98]

Let us now see whether the way in which the procedure followed by technique to create the legal rule is structured can be a valid substitute for the lack of political-representative legitimation and thus compensate for the absence of an electoral mandate.

[98]A. Cardone, "Decisione algoritmica" vs Decisione politica?, cit., 163.

Regardless of the procedure chosen, it has been argued with suggestive reasoning[99] that the process alone would guarantee the goodness of the final rule, thereby making up for technique's inability to represent and synthesise political interests and demands. We propose a different idea: the succession of preliminary moments that are correct in themselves is not enough to ensure the common good. The neutrality of the procedure does not automatically result in the victory of good over evil, because its output depends on how the person has oriented, guided and finally verified the technique. Thus, proceduralising technique[100] does offer one certainty: obedience to a pre-packaged process before it begins. This is not a small matter, but it does not deserve improper meanings. If overvalued, procedure, reduced to an empty shell, is promoted to a source legitimising the future rules it will give itself.

In the long run, this proceduralisation distracts from the political knots hidden beneath procedural perfection: the defence of the separation of powers and of fundamental freedoms. Their protection must instead remain entrusted to the representative political subject, which has the duty to act personally to guarantee them to its citizens, refraining from delegating the task to pale substitutes incapable of delivering a result.

We note that the hyper-technological context cuts the legs out from under the rule of law. The division of powers yields before an omnipotent technique, the new Sun King of the digital age, which behaves as legislator and also as administrator and, where necessary, even as judge, thanks to the in-house adjudication tested by many platforms. Nor have fundamental freedoms received better treatment in terms of legal certainty, because they are protected if, and to the extent that, they coincide with the mechanistic rules that technique dictates from time to time according to statistical repetition. Therefore, the protection of freedoms is entrusted to an entirely future and uncertain event, whose occurrence will depend on their occasional coincidence with the private objectives of regulatory authorities: "may claim that their objective are in line with the

[99]Contra: O. Pollicino, Regolazione e innovazione tecnologica nell'ordinamento della rete, in Riv. AIC, 2, 2025, 152.

[100]E. Celeste, Digital Constitutionalism: a new systematic theorisation, in Int. Rev. L. Comput. Treaty, 2019, 33, 76; and G. De Gregorio, The Normative Power of Artificial Intelligence, in Ind. Jour. Glob. L. S., 2023, 30, 73.

public interest, but whether or not this is so will depend on the frameworks in which they operate".[101]

In conclusion, this unconditional trust in the salvific power of procedure is not only unsupported by real evidence but also prejudices the stability of the legal order, because "procedural fetishism"[102] — that is, the uncritical flattening on the thaumaturgic virtues of a process closed in its formal perfection[103] but light in content — places both the care of our freedoms and the limits on constituted powers in the uncontrolled hands of AI, in the illusory hope that "if we manage to do so just procedures will yield just outcomes".[104]

Finally, let us reflect on the impact of technique on the system of sources of law. It breaks with the principle of hierarchy among sources, since it is difficult to maintain that the technical rule, perfectly coinciding with AI, is placed on a step immediately below the European Regulation, filling its blanks. Reality is far from this theoretical construction because technique has further diversified the scale of sources by adding a new step: beyond the State and beyond private authorities. This is a fictio iuris that must not deceive us, because technique absorbs politics, overwhelms it and, supported by a licence of legitimacy, issues ad personam and concrete determinations obeying statistical logic, which have nothing in common with the free choice of values reserved to the political decision-maker.

Let us now ask whether this concrete provision by AI in place of abstract regulation creates problems for the legal order, continuing the reasoning just concluded on sources. As a result of technique, the legal order will tend to approach common-law models, with the peculiarity that the stare decisis of judicial decisions will be replaced by the automatic determination of the artificial mind, with effects preventing legal

[101] J. Kay - J. Vickers, Regulatory reform: an appraisal, in G. Majone (ed.), Deregulation or re-regulation? Regulatory reform in Europe and the United States, London, 1990, 239.

[102] T. R. Tyler - K. M. McGraw, Ideology and the interpretation of personal experience: procedural justice and political quiescence, in Jour. Soc. Issue, 1986, 42, describe procedural fetishism as a dangerous tendency leading people to believe that an unjust decision is correct merely because it obeys strict formal rigour.

[103] J. Rocheleau, Proceduralism, in D. K. Chatterjee (ed.), Encyclopedia Global Justice, Salt Lake City, Springer, 2012, 906.

[104] E. Ceva, Beyond legitimacy. Can Proceduralism say anything relevant about justice?, in Critical Rev. Int'l Soc. and Pol. Phil., 15, 12, 2012, 183–191.

innovation. Whereas the judge may, under certain conditions, overturn previous decisions because new values have emerged, AI is not trained in overruling. Consequently, the biased rule will crystallise, reproducing the same error for the future, now no longer removable. [105]

In conclusion, technique as source commits several violations of law in a single move: it tramples on the hierarchy of sources, wears down legal certainty, denies the legal order the attribute of civil law, perpetuates injustices for the future and masks everything with fake legality.

In short, this technique cancels the democratic value of the rule of law in favour of the arbitrariness of the rule of tech. [106]

8.9 Looking to the future

What prospect is there for the relationship between Technology and Politics?

We propose an ancient rule: to each its own. The old — the norm that exhausts in itself every manifestation of juridicity — and the new — technique that is eroding the terrain of the former, not always lawfully — must be composed within a networked structure of the legal order that reserves to the supranational political subject the task not of regulating human conduct in detail, but of ordering multiplicity, bringing diversity back to unity; in short, of "réaliser la mise en cohérence" and ensuring the compatibility of norms of different origin.

Thus it is for the politics of European representative subjects to design ex ante the structure and interaction of the private systems to be controlled and developed so that they can integrate the larger legal order through self-regulation. Hence an order of intervention: the diffusion of normative power among the new beneficiaries — independent authorities, private interest governments and Technique — must not be left to itself, but outlined by the political decision-maker in the subjective and functional profile of the new authors, identifying specific objectives and values to be

[105] F. Donati, Intelligenza artificiale e giustizia, in Riv. AIC, 1, 2020, 421; E. Longo, Giustizia digitale e Costituzione. Riflessioni sulla trasformazione tecnica della funzione giurisdizionale, Milan, Franco Angeli, 2023; and the author's Giustizia e intelligenza artificiale: un equilibrio mutevole, in Riv. AIC, 2, 2024, 95 ff.

[106] M. Zalnieriute, Against procedural fetishism: a call for a new digital constitution, in Ind. Jour. G.L.S., 39, 2, 2023, 253–256.

pursued through their future rules. This division of labour preserves for the supranational political subject its indispensable responsibility to recompose imperative and consensual law into a system; while allowing the new regulators to continue, not to start ex novo, the political discourse already set in its main lines by the first actor who preceded them.

A legal order that tends to be articulated across several legal spaces, acting simultaneously and intervening on the same objects with different force, has one single point of tension: orienting each legal reality to respect the value heritage of every other. This means, on the one hand, avoiding — by establishing measures of reciprocal tolerance — the mutual annihilation of the ideals of regulatory subsystems and, on the other, guaranteeing the coherence of the law produced by the new authors with the supreme values of the political order, for which Europe is ultimately responsible.

Therefore, the only mode of cooperation between traditional imperative sources and the others — public, private and mechanical — lies in the complementarity of the latter to the former, the only ones capable of combining the plurality of derived orders with the superiority of the original order. That original order may well make use of endogenously generated rights, provided it indicates to them ex ante the direction to take and intervenes ex post to correct any outcomes incompatible with the guidelines given.

The supranational legislator will therefore have to do less and do it differently than it has done so far.

As to doing less, it will have to eliminate rules overtaken by a reality that has moved on; rules uselessly invasive of business autonomy that bring no benefits to the contestability of digital markets; discriminatory rules that weigh more on small actors and less on large ones; and rules that misalign situations that should be treated equally in the presence of the same service provided by alternative means. Doing less will also concern procedures designed for national and European authorities that act autonomously from one another, preferring constructive dialogue — rather than solipsism that then becomes confusion of procedures and disciplines — in order to design rules few in number but plural in their values.

As to doing differently, the legislator will have to rewrite part of the AI discipline to correct its egoistic torsion, caused by the improper use of self-declarations instead of impartial public controls, which are more suitable than the former for ensuring substantive, not presumed, compliance with the precautionary rules laid down to protect the fundamental rights of the person. This attention to the individual would mark the beginning of a digital humanism that is not merely a linguistic expression forgotten in a recital, but a value that becomes a rule of relationship between Politics and Technology. The latter is no longer at the service of strong and well-endowed private groups, but stands alongside citizens and their expectation of relying on a technique that hides no traps behind apparent legality, that is understandable in its logical path and that tries to improve the life of those — individuals or communities — who have been left behind.

A similar operation should be carried out on the many DMA rules, which should be thinned out and rewritten, privileging concrete assessments of dominance over typical legal assessments. This regulation, relieved of the attribute of permanence, should withdraw once competitive balance is achieved. The whole should be completed by a sanctioning system courageous in its structural remedies, those that break up the vertically integrated operator, and redesigned in its pecuniary penalties, today almost welcome caresses to the Tech Barons, leaving them undisturbed in their dominance.

Only under these conditions could the intertwining of Technology and Politics, from an encounter that objectively disaggregates the legal order, come closer to being a factor of growth for the legal order and become a place deserving of citizens' trust, because it would be counterbalanced by the presence of a strong political decision-maker, architect of the system and, at the same time, regulator of last resort.

9 Conclusions: regulation and governance in the age of generative AI

Andrea Renda

The regulatory framework on artificial intelligence that is consolidating at European level is the product of an extraordinarily intense legislative season, characterised by an unprecedented effort to anticipate the risks of a rapidly evolving technology. The AI Act, the DSA, the GDPR and the Digital Omnibus proposal, among others, make up a complex legal mosaic, whose coherent application depends decisively on the quality of enforcement at national level and on the ability of sectoral authorities to interpret their role in a proactive and adaptive manner.

In the face of this complexity, the chapters of this Report converge on a common message: AGCOM cannot simply wait for the regulatory framework to stabilise before taking action. The window of opportunity to build internal technical capacity, forge institutional alliances and acquire legitimacy as an AI regulator is open now, and risks closing rapidly if it is not seized decisively.

9.1 Prospects for the application of the AI Act and the DSA

The process of applying the AI Act is proceeding at a much slower pace than hoped. The postponement to August 2027 of the rules relating to high-risk applications — decided within the framework of the Digital Omnibus proposal — and the difficulties in completing the standardisation work entrusted to CEN-CENELEC leave open a long phase of regulatory uncertainty. During this interval, the DSA remains the main reference instrument for the enforcement of content generated or amplified by AI on digital platforms. AGCOM — in its capacity as Digital Services Coordinator — is already called upon today to exercise supervisory and sanctioning powers that have a much broader scope than the public debate has so far recognised.

If translated into law in the form currently proposed by the Commission, the Digital Omnibus will introduce significant centralisation of AI enforcement in the hands of the

AI Office, especially for systems developed from GPAI or used by large platforms. This scenario will make it even more urgent for AGCOM to position itself as a credible interlocutor of the AI Office and as the reference authority for national contexts of AI application in the sectors falling within its competence.

9.2 The pervasive nature of AI and AGCOM's regulatory competences

One of the most relevant contributions of this Report is the demonstration — through the systematic mapping in Chapter 3, and in even greater detail in the annex — that artificial intelligence is not a sectoral phenomenon but a cross-cutting paradigm that runs through all areas of AGCOM's competence. Algorithmic management of electronic communications networks, personalisation of media content, protection of pluralism and consumer protection in interactions with automated systems: these are not separate challenges, but different expressions of a single transformation that requires an equally unified regulatory response.

This cross-cutting nature has precise practical implications. First, the challenges of AI cannot be addressed with tools designed for a single sector: what is needed is a modular regulatory framework capable of translating common principles — transparency, human oversight, non-discrimination, protection of vulnerable persons — into operational obligations specific to each context. Second, AI supervision requires interdisciplinary technical capacity that cannot be improvised: the comparative benchmark with Ofcom, Arcom and BNetzA shows that authorities that invested early in data scientists, AI auditors and internal technical laboratories achieve significantly better enforcement results. Third, coordination with other national authorities — the Data Protection Authority, AGCM, ACN — is not an institutional optional extra but a structural condition for the effectiveness of the system.

9.3 Generative AI and agentic AI: new regulatory frontiers

The rapid evolution towards "agentic" AI systems — capable of operating autonomously, planning complex actions and interacting with the digital environment without continuous human supervision — raises radically new questions for the

application of the AI Act and for the role of sectoral authorities. Agentic systems challenge the fundamental premise of the risk-based approach: the identifiability and predictability of use cases. An autonomous agent that negotiates contracts, generates content, manages network infrastructure or interacts with consumers performs functions that simultaneously fall within multiple risk categories and multiple areas of regulatory competence.

For AGCOM, this means preparing for scenarios in which LLMs and AI agents operate as autonomous actors in the media and communications ecosystem: producing content, managing social-media accounts, personalising commercial offers and moderating online discussions. The regulatory response cannot wait for completion of the European legislative framework: the development of specific guidelines, notification protocols and audit systems adapted to this new generation of systems must begin now.

9.4 Regulating with AI: SupTech and adaptive governance

This Report does not merely analyse how to regulate AI, but opens an equally relevant perspective: how to use AI to improve the quality of regulation itself. Supervisory technology (SupTech) — from automated data-traffic monitoring systems to semantic-analysis tools for detecting disinformation — can radically transform AGCOM's enforcement capacity, enabling a shift from periodic audits to continuous monitoring and from ex post interventions to anticipatory responses.

The perspective of "law as code" — in which rules are formalised computationally and applied automatically — is still far from the reality of Italian and European regulation, but it represents a trajectory towards which investments in technical capacity and institutional expertise should be oriented. An authority that knows how to use AI to regulate will also be an authority better equipped to regulate AI.

9.5 Towards European technological sovereignty: the EuroStack and AGCOM's role

The geopolitical context in which AGCOM is called upon to act is marked by a structural tension between Europe's dependence on large AI models developed in the United

States and China, and the ambition to build a sovereign technological infrastructure — the so-called EuroStack — capable of guaranteeing resilience, pluralism and respect for fundamental European values. In this context, independent authorities such as AGCOM are fundamental actors: not only as guardians of compliance with the rules, but also as active promoters of an innovation ecosystem that is both competitive and worthy of citizens' trust.

9.6 A digital social contract for the age of AI

The thread running through all chapters of this Report is the conviction that technology is not neutral: artificial intelligence, like every other form of power, requires democratic legitimacy and public accountability. Independent authorities — created to protect the general interest from distortions of markets and private powers — are now called upon to perform this function in a digital ecosystem where asymmetries of power, information and capacity have multiplied exponentially.

Ultimately, this Report is a contribution to the construction of a "digital social contract" for the age of AI: a pact between institutions, businesses and citizens that recognises the extraordinary benefits of technology, but does not give up governing its risks with proportionate, effective tools that respect fundamental rights. AGCOM can and must be one of the protagonists of this process, contributing its sectoral expertise, institutional independence and capacity for dialogue with European and national actors in the AI governance system.

9.7 Main recommendations

On the basis of the contributions collected, the Committee formulates the following priority recommendations for AGCOM:

- **Strengthening internal technical capacity:** Invest in a dedicated team of AI auditors, data scientists and specialised lawyers capable of conducting autonomous algorithmic inspections and developing independent testing tools modelled on the experiences of Ofcom and BNetzA. The team should be structured as a cross-cutting unit, with expertise in reverse engineering of recommendation algorithms, analysis of bias in datasets and assessment of the compliance of AI systems with the obligations of the AI Act. The initial investment should prioritise

the recruitment of senior technical profiles and the conclusion of agreements with universities and research centres, following the model of Ofcom's Data Science Lab and the partnership between Arcom and France's INRIA.

- **Strengthened institutional coordination:** Conclude formal cooperation protocols with AgID, ACN, the Data Protection Authority and AGCM, ensuring coherent and proportionate enforcement of the European regulatory framework on AI in the respective areas of competence. The protocols should provide for concrete operational mechanisms: permanent technical tables for managing cases of overlapping competences, reciprocal notification procedures when proceedings involving AI systems are opened, and a shared system for users to report infringements. The objective is to overcome the risk of fragmentation that would make the entire enforcement system ineffective, preventing regulated entities from exploiting coordination gaps between authorities.
- **Establishment of a permanent AI Observatory:** Create a system for continuous monitoring of the impacts of AI in regulated sectors, with public dashboards, periodic reports and automated detection tools for bias, discrimination and violations of information pluralism. The Observatory should operate quarterly, publishing a public report on a set of standardised indicators — including the diversity of content promoted by recommendation algorithms, concentration in the advertising market, throttling and zero-rating practices in data traffic, and cases of deepfake detected in political communications. The model is Arcom's Observatoire des algorithmes, which has shown that permanent monitoring produces deterrent effects significantly greater than periodic audits.
- **Adjustment of the sanctioning system:** Activate the sanctions provided for by the DSA (up to 6% of global turnover) and by the AI Act (up to 7%), overcoming the structural limits of Law No. 249/1997, which make enforcement insufficiently deterrent in relation to operators' turnover. The adjustment requires legislative intervention updating the maximum penalties provided for by AGCOM's founding law, harmonising them with European thresholds and ensuring proportionality with respect to the economic size of regulated entities. In parallel, sanctioning procedures should be reformed to reduce the time required to conclude

proceedings and to introduce the possibility of immediate precautionary measures in cases of systemic risk, preventing the slow course of procedures from neutralising the deterrent effect of sanctions.

- **Development of a modular regulatory framework:** Draw up sectoral codes of conduct, guidelines and algorithmic-transparency obligations harmonised across the different areas of competence, based on common principles adaptable to technological evolution: transparency, human oversight, non-discrimination and protection of vulnerable persons. The framework should be structured on three levels: a set of horizontal principles valid for all regulated sectors; specific obligations tailored to each area — electronic communications, audiovisual media, postal services and consumer protection; and an annual review mechanism incorporating evidence emerging from the Observatory and developments in the European regulatory framework. This approach makes it possible not to multiply regulatory instruments, but instead to design them once with the necessary care and make them adaptable to different application contexts.
- **Active participation in European networks:** Contribute proactively to BEREC and ERGA working groups, co-constructing common tools for AI auditing and the harmonisation of enforcement practices at European level. In these contexts, AGCOM should present itself not as an actor receiving instructions, but as the bearer of specific regulatory experience — that of Digital Services Coordinator in a large country — and as a promoter of acceleration in the development of shared standards. In particular, participation in the BEREC AI Toolkit and in ERGA work on deepfakes and algorithmic pluralism offers the opportunity to influence the European standards that will also apply to the Italian market, with significant competitive advantages for an authority that has already developed internal technical capacity.
- **Experimentation and SupTech:** Launch experimentation with supervisory technology (SupTech) tools for automated monitoring of regulated markets, opening the way to forms of enforcement based on real-time data rather than periodic inspections. AGCOM should establish a regulatory sandbox dedicated to AI systems operating in the sectors within its competence — electronic

communications, audiovisual media, digital and postal services — enabling businesses, start-ups and research centres to test innovative solutions in a controlled environment, with temporary and circumscribed derogation from ordinary regulatory obligations. The reference model is the one already provided for by Article 57 of the AI Act for national competent authorities, which AGCOM could activate in coordination with AgID and ACN, positioning itself as the first Italian regulatory laboratory on AI applied to the media and communications ecosystem.