Shaping Europe's Digital Future Through a Change of Perspective: The Necessary Rethinking of the Relationship Between Regulation and Innovation in the EU

Edoardo Raffiotta*

ABSTRACT: The paper analyzes the EU's digital regulatory framework and argues that its rapid expansion has generated significant multi-regulatory and multi-level enforcement challenges. Overlapping rules and fragmented authorities undermine legal certainty, increase compliance burdens, and risk discouraging innovation and investment. The paper calls for a recalibration of Europe's digital governance through a Charter-centred balancing of fundamental rights, clearer coordination among regimes, and the use of adaptive regulatory tools. It proposes a model of multi-level economic constitutionalism that aligns legal coherence, institutional simplification, and material investments, enabling the EU to sustain a competitive, innovation-oriented and rights-compliant digital ecosystem.

KEYWORDS: digital constitutionalism; AI; over-regulation; Brussels effect; regulatory overlap

1. Preliminary Overview

In 2019, the European Union launched its digital strategy, aimed at building a Europe "fit for the digital age" in what had already been dubbed the "Digital Decade".[1]

The objectives of the European Strategy are well known and can be summarized in three bullet points: promote (and increase) innovation; at the same time, limit the risks connected with the development, dissemination, and use of new digital technologies;[2] while strengthening (or building?) European technological sovereignty.

* *Associate Professor of AI and Constitutional Law, University of Milan-Bicocca.Mail: edoardo.raffiotta@unimib.it.*
The article was subject to a double-blind peer review process.

[1] See A. BRADFORD, *Effetto Bruxelles. Come l'Unione Europea regola il mondo*, tr.it., Milano, 2021; as cited also in T.E. FROSINI, *L'orizzonte giuridico dell'intelligenza artificiale*, in *BioLaw Journal – Rivista di BioDiritto*, Online First, 2022.

[2] See A. D'ALOIA, *Il diritto verso "il mondo nuovo". Le sfide dell'Intelligenza Artificiale*, in *BioLaw Journal – Rivista di Biodiritto*, 1, 2019, 3-31, for a broad view of the legal implications of the AI systems' development, from the responsibilities related to these new forms of behavior, to the risks linked to the profiling and micro targeting of people.

On closer inspection, those objectives had already appeared in the European agenda well before the launch of the Digital Strategy. Numerous Recitals and Articles of the GDPR mention them (expressly or implicitly): from Recital 7 (which stresses the need to create trust to enable the development of the digital economy in the internal market), to Recital 71[3] and Recitals 75–77 which, together with Article 1 of the Regulation, combine the well-known risk-based approach with safeguarding the free flow of data – thereby identifying risk assessment as the GDPR's structural point of equilibrium – through to objectives linked to the internal market (for example Recitals 10 and 13).

Ten years after the first publication in the EU's Official Journal of Regulation 1679/16, and more than five years after the inauguration of the Digital Strategy, it is possible to draw an initial balance of European action; amidst light and shade.

On the one hand, the Union has invested a substantial amount of resources in this endeavor (first and foremost, financial: the Court of Auditors estimates the EU's financial allocation for the digital ecosystem, 2021-2027, at 235 billion euros).[4] The regulatory infrastructure has been significantly enriched, and today covers (*rectius*: claims to cover) almost every declension of the digital phenomenon: following the GDPR came the Digital Services Act and the Digital Markets Act, the Data Governance Act and the Data Act, the Union's Cybersecurity Regulation (not forgetting the NIS Directives), up to the AI Act, together with numerous measures devoted to specific sectors considered high-risk (such as healthcare, through the European Health Data Space; or finance, through the various measures of the so-called Digital Finance Package), without forgetting initiatives that will apply in the future (e.g., the Cyber Resilience Act, and more). The European legislator's objective is, once again, crystal clear: to protect, ultimately, consumers – the end recipients of digital technologies – even when that protection necessarily entails regulation (and hence limitation)[5] of technological development. And this, above all, in light of competitors such as the United States and China (with respect to which the EU has by now amply shown that it intends to adopt a human-centered approach, explicitly oriented to the protection of freedoms and individual rights,[6]

[3] C. CASONATO, *Intelligenza artificiale e diritto costituzionale: prime considerazioni*, in *DPCE Online*, 2019, was already highlighting the importance of Recital 71, primarily as a basis for establishing the right to a human decision.

[4] https://www.eca.europa.eu/ECAPublications/SR-2025-13/SR-2025-13_EN.pdf, 8.

[5] A. PAJNO *et al*., *AI: profili giuridici. Intelligenza Artificiale: criticità emergenti e sfide per il giurista*, in *BioLaw Journal – Rivista di BioDiritto*, 3, 2019, 205-235, on the need to foster technological developments and that of protecting fundamental rights.

[6] In particular, when it comes to regulating the digital phenomena, the EU seems to express a systemic preference, or at least a tendency towards greater protection, in favor of so-called "freedom rights" (freedom of expression; right to confidentiality and privacy; et al.) over so-called "economic rights." This tendency was already clearly evident in the well-known leading case *Google Spain* (C-131/12) and it has since been further reinforced, as demonstrated by the *Schrems I* (C-362/14) and *Schrems II* (C-311/18) cases. More recently, see the *Glawischnig-Piesczek v. Facebook Ireland* case (C-18/18). It is clear that, according to EU case law, the freedom to conduct a business, although guaranteed by article 16 of the Charter, is not an absolute right and may be legitimately restricted (as is often the case) in order to protect other fundamental rights such as dignity, privacy, and freedom of information. And this, as we shall see, carries the risk of having negative repercussions on the European single market.

seeking to distinguish itself from realities – such as the U.S. and China – which are more attentive, albeit in extremely different ways,[7] to market implications).[8]
On the other hand, European (hyper-)production of rules is not exempt from criticism. In our view, the main criticalities of European action can be grouped around two main categories: multi-regulatory concerns and multi-level enforcement concerns.

1.1. Multi-regulatory concerns

One of the most critical challenges for any legislator is to strike a balance between, on the one hand, the regulatory intent[9] and, on the other hand, the slippery slope of over-regulation. Toward which, it is now possible to affirm with certainty, the European Union is sliding.[10]
By '*multi-regulatory concerns*' we refer to all potential critical issues that may arise from the presence of an excessive number of legislative acts and regulatory instruments within the Union's regulatory framework: we designate the range of potential challenges emerging from an overabundance of legal norms and instruments, understood primarily in *quantitative* terms.
This is evidenced, first, by the volume of legislative production originating in the Union in recent years. Even more so since, in addition to the Union's own acts, one must also recall all those national acts that are a direct consequence: transposition acts (for directives), or implementing acts, or harmonization acts,

[7] It is now well known that the US adopts a purely market-oriented approach focused on freedom of innovation, while China makes extensive use of technology in state-citizen dynamics. For an overview of one of the main risks associated with this approach, see G. CERRINA FERONI, *Intelligenza artificiale e sistemi di scoring sociale. Tra distopia e realtà*, in *Il diritto dell'informazione e dell'informatica*, 1/2023, 1-24.
[8] For a comparison of different models and perspectives on regulating the intersection between AI and privacy, see R. TARCHI, *Intelligenza artificiale e protezione dei dati personali: problemi di metodo e di procedura*, in *DPCE Online*, 2024.
[9] See also A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal – Rivista di BioDiritto*, 1, 2019, 63-89, on the inherent tension between AI and constitutional law.
[10] I already discussed this topic in E. C. RAFFIOTTA, *Dalla self-regulation alla over-regulation in ambito digitale: come (e perché) di un necessario cambio di prospettiva*, in *Osservatorio Sulle Fonti*, 2023, 245-267.

as well as national legislation (primary and secondary) destined to interact with EU regulation.[11] It is evident that if regulating is mandatory, regulating too much (or badly)[12] can become deleterious.
This results in greater interpretive – and consequently – enforcement difficulty[13] (see *infra*) and greater and avoidable compliance costs and burdens (whose most significant impact falls – as well shown by the recent Draghi Report – on small players, introducing genuine artificial regulatory barriers to market entry[14]). Recent reports, such as the Letta Report, the aforementioned Draghi Competitiveness Report, and the European Commission's own GDPR review, have highlighted the urgent need for regulatory reform to maintain (and reinforce) Europe's digital competitiveness. Compliance costs for SMEs can reach up to 12% of revenues, compared to 5% in the US, and 40 out of 141 European unicorns have relocated abroad since 2008. These figures underscore the direct link between regulatory complexity and barriers to innovation and investment; thus paradoxically having opposite effects to those the Union's Digital Strategy seeks to achieve, as already flagged by the Financial Times).[15] We then have to deal with cumulative risks (which, not by chance, the Union has already identified[16] as one of the elements to be considered in measuring

[11] A prime example is – in the case of Italy – the regulatory framework on cybersecurity: in addition to European regulations (NIS and NIS2; European Cybersecurity Regulation), it is important to remember the introduction by Decree Law 105/2019 of the National Cyber Security Perimeter, to ensure a high level of security for the networks, information systems, and IT services of public administrations, entities, and public and private operators based in Italy, on which the exercise of an essential function of the State depends; as well as Prime Ministerial Decree 131/2020, which identified the parameters for identifying entities that perform essential functions or provide an essential service for the State; while Prime Ministerial Decree 81/2021 identifies, through the attached tables, the categories of incidents that have an impact on ICT assets. The classification is then used to identify the timing of communications to the CSIRT that the regulation requires from entities identified within the security perimeter. Presidential Decree No. 54/2021 identifies the procedures, methods, and terms to be followed for the acquisition of supplies by entities included in the perimeter, while the subsequent Prime Ministerial Decree of June 15, 2021, identifies the categories of ICT assets intended for use within the national cyber security perimeter. while Prime Ministerial Decree No. 92 of May 18, 2022 establishes the procedures, requirements, and terms for the accreditation of accredited testing laboratories (so-called LAPs) in support of the National Evaluation and Certification Center (CVCN).
[12] On this point, for a national perspective, see M. BARONI, *Se la Corte si fa (giocoforza) legislatore. Alcune considerazioni intorno a Corte cost. n. 110/2023*, in *Federalismi.it*, 19/2024, in which the Author examines the importance of constitutional powers and loyal cooperation between institutional actors as the foundation for the efficiency of the constitutional state, in a systemic context in which transnational forces weaken the traditional institutional structure, thus highlighting the decline of the legislative role of Parliament.
[13] It should also be borne in mind that, naturally, the EU legal framework is constantly evolving, partly as a result of interpretations not only crystallized in court rulings but also in the activities of the EU institutions themselves: consider, for example, the Commission's decision, published on July 10, 2023, on the adequacy of the EU-US Data Privacy Framework (the new regulatory framework for the transfer of personal data between the EU and the US). In this decision, the Commission found that the level of protection offered by the US for data transfers from the EU is comparable to that of the EU and, therefore, acceptable; However, neither the Parliament (https://www.europarl.europa.eu/doceo/document/TA-9-2023-0204_EN.html) nor the European Data Protection Board (EDPB - https://edpb.europa.eu/news/ news/2023/edpb-welcomes-improvements-under-eu-us-data-privacy-framework-concerns-remain_en): making it highly likely that the matter will be referred to the Court of Justice of the European Union.
[14] "We claim to promote innovation, but we continue to add regulatory burdens to European companies, which are particularly costly for SMEs and self-defeating for those in the digital sectors". Draghi Report, Part A, 4.
[15] Financial Times, *European companies sound alarm over draft AI law*, June 29, 2023.
[16] EU Commission, *Better Regulation Guidelines*, Nov. 21st, 34 e 40.

the effectiveness of an impact assessment) and with the (negative) effects on investment and, prospectively, on innovation itself:[17] in simple words, the risk (which by now seems a certainty) is that in the European Union it is increasingly complex to innovate (and consequently increasingly challenging to find those willing to invest in Europe).

Finally, as will be discussed in more detail below, the presence of multiple sources inevitably produces phenomena of regulatory overlapping (which – even in theory – the Union is aware it must avoid, as expressly indicated in Smart Regulation in the European Union).[18]

From a constitutional perspective, multi-regulation does not only denote an excess in the number of acts, but a weakening of normativity itself.[19] When the same technological process is simultaneously captured by partially overlapping regimes (GDPR, DSA, DMA, Data Act, AI Act, NIS2, MDR, EHDS, sectoral lex specialis), the addressee's duty of compliance becomes structurally indeterminate: the norm loses its capacity to orient behaviour ex ante and is transformed into an ex post bargaining space between authorities and regulated entities. This "regulatory density without hierarchy" undermines the principle of legal certainty[20] and indirectly erodes the effectiveness of fundamental rights, which presuppose predictable constraints and knowable balances. The Draghi report, as well as the State of the Digital Decade 2025, converges on this point: regulatory fragmentation and cumulative burdens represent a competitiveness constraint in themselves, forcing European operators, especially SMEs, to internalize structural uncertainty as a cost of staying within the Union's legal space. In this sense, multi-regulatory concerns are not a merely technical pathology; they signal an asymmetry between the Union's ambition to project regulatory power and it's still fragile capacity to produce coherent, systemically integrated discipline.

1.2. Multi-level enforcement concerns

A second and less evident – but no less important – effect of European over-regulation is the Union's growing difficulty in achieving an *organic application* of its regulatory output: it is worth recalling that the Digital Single Market Strategy, introduced in 2015 by the Juncker Commission[21], has been rapidly identified as one of the flagship priorities of the European Digital Agenda and has been later incorporated into the framework of the Digital Decade 2030.[22] Also, we must not forget that the European Union itself specifies that proper application of EU law requires structured cooperation with (and among) the Member States and a strategic approach to enforcement, thus signaling the inherently multi-level nature of the European regulatory ecosystem.[23]

---

[17] "Up to 30% of EU tech companies resources can be taken up by compliance instead of focusing on the company's growth and innovation" according to the European Tech Alliance.

[18] (COM(2010) 543 final), in https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52010DC0543.

[19] F. Faini, *Intelligenza artificiale e diritto: le sfide giuridiche in ambito pubblico*, in *BioLaw Journal – Rivista di Biodiritto*, 1, 2019, 145-162, highlights that the technological approach alone is not enough, but it must be guided by the ability to direct the technique by means of law.

[20] G. De Minico, *Diritti regole Internet*, in *Costituzionalismo.it*, 2, 2011, pointed out, with regard to network regulation, that the plurality of regulatory instruments raises the question of the existence of an order among them, and the example already indicates a possible criterion for clarifying who should intervene first and who second.

[21] COM(2015)192 final (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192).

[22] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022D2481.

[23] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017XC0119(01), 2.

By the notion of '*multi-level enforcement concerns'* we refer to the derivative challenges that emerge *from* the overproduction of regulatory norms within the Union. The focus is thus not merely on their numerical proliferation, but on the interpretative and enforcement complexities generated by such normative abundance – whereby a quantitative excess ultimately translates into a qualitative weakness of legislation.

In particular, this phenomenon manifests in two different forms: vertically and horizontally.

When talking about the "vertical" dimension, we refer to the relationship between the European Union and the Member States: when compliance obligations on a given topic are contained among different acts, national transposition may be incomplete or slow, creating legal uncertainty and differences between countries (for example, on May 7, 2025 the Commission sent reasoned opinions to 19 Member States for failure to fully transpose the NIS2 Directive).[24] The same also happens when one subject matter is regulated by multiple sets of rules of different types (even more so if they belong to different periods and therefore have different approaches). This is the case for privacy: on the one hand, the GDPR and all the individual national harmonization measures; on the other hand, the ePrivacy Directive, whose reform – despite increasingly evident reform needs (to which we return *infra*) – has remained, since 2023, at the EDPB's guidelines on tracking techniques covered by Article 5 of the same ePrivacy Directive.

When talking about the "horizontal" dimension, we refer to relations among the Member States. One cannot fail to note that the current state of the Union's regulatory apparatus has clear (negative) effects also within the Member States: indeed, precisely the different modes and timings of transposition (or application) mentioned above make *inter-state* divergences far from uncommon (for example, on market access); thus creating an environment in which it is becoming increasingly difficult to build a cross-culture of compliance.[25]

All this creates fragmentation in the internal market which, obviously, constitutes a further obstacle to the persistence of investments and investors (althought the Union is fully aware of this: the State of the Digital Decade 2025 report[26] expressly mentions fragmentation in the internal market as one of the most significant obstacles to innovation,[27] while indicating simplification and reduction of administrative burdens as a necessary path toward a more innovative and competitive European market).

In addition, we can identify two further criticalities that impact both vertically and horizontally.

The first problem concerns the authorities.

On the one hand, norms' over-production over the last decade has led to the proliferation of authorities responsible for supervision, enforcement or interpretation of rules. Regarding the GDPR, its enforcement architecture remains highly fragmented, with one DPA per Member State (plus the EDPS and EEA

[24] https://digital-strategy.ec.europa.eu/en/news/commission-calls-19-member-states-fully-transpose-nis2-directive.

[25] See Noyb, European Center for Digital Rights, *GDPR: a culture of non-compliance? Numbers of evidence-based enforcement efforts*, 2024: based on a large-scale survey conducted in November 2023 among 1,048 data protection professionals – mainly Data Protection Officers (DPOs) working in medium and large enterprises across the EU/EE – the study concludes that the GDPR has increased awareness of privacy but failed to establish a genuine european culture of compliance. The gap between legal norms and business practice persists also due to insufficient and uneven enforcement among the Member States (also considering organisational resistance and a risk-based corporate logic whereby non-compliance remains economically rational).

[26] Communication from the Commission '*State of Digital Decade 2025: Keep building the EU's sovereignty and digital future*' (main report), 17.

[27] *Ibid*., 9.

observers) and a multi-layer set of local or regional authorities (16 Länder DPAs, plus the federal BfDI): a structure that encourages divergent procedures and outcomes and weakens *ex post* accountability across borders. In more practical terms, the one-stop-shop has struggled to deliver timely, coherent cross-border outcomes, failing on governance and accountability. The same is happening with the AI Act, which has led to the birth of a new centralized entity (the AI Office; Article 64), in addition to the individual authorities of the Member States (Articles 28–39, 88–94; in Italy, two)[28], as well as three advisory bodies (the European Artificial Intelligence Board; the Scientific Expert Group; and finally the Advisory Forum, representing a diverse selection of stakeholders, both commercial and non-commercial; Articles 65–67, 70–72).

On the other hand, this entails greater difficulties for practitioners (not infrequently it is difficult to know which Authority to deal with),[29] and more frequent coordination difficulties between Authorities: we need to think, for example, of possible divergent interpretations of the same provision or – even worse – possible conflicts of competence. It is therefore unsurprising that, in such a complex context, even Article 60 of the GDPR, dedicated precisely to cooperation between supervisory authorities (the article introduced, as is well known, the concept of the one-stop shop, one of the Regulation's main innovations), required dedicated interpretive guidelines.[30]

The second (further) problem is represented by cross-regulatory consistency: in digital sectors such as privacy, content, competition, and cybersecurity, it is essential to ensure that the various obligations applicable to the same process or service are fully aligned. Given the pace of technological evolution, *regulatory clarity* and *interpretative coherence* – and thus the speed of practical implementation – are more critical in this areas than in any other.[31] In the European context, this appears to be increasingly difficult:[32] it is no coincidence that the 2023 Commission proposal for a GDPR Procedural Regulation and the subsequent Parliament briefings aim to harmonize cross-border complaint handling, tighten cooperation timelines, and thereby reduce inconsistent application (views on the Commission proposal diverge: while some advocate for enhanced complainant rights, an equal say for the lead supervisory authority and the supervisory authorities concerned on the substance of enforcement decisions; others highlight the need for a stronger role for the LSA and lesser roles for the CSAs and the EDPB.[33] This solution seems to be preferable,

[28] Article 20 of the National AI Law (L. 132/2025), implementing Article 70 of the AI Act, designates two entities as national authorities for artificial intelligence: the Agency for Digital Italy (AgID) and the National Cybersecurity Agency (ACN).

[29] As regulations governing the data economy increase, so do the number of authorities involved and the risk of overlap between multiple competent authorities, without any clear procedure to refer to, both for the authorities themselves and for the companies and public administrations directly concerned, as well as for citizens who have the right to be protected.

[30] https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-022022-application-article-60-gdpr_en.

[31] It is no coincidence that the EDPB has expressly called for inter-regulatory consistency and cooperation with other authorities in the GDPR assessment/enforcement cycle (https://www.edpb.europa.eu/our-work-tools/our-documents/statements/statement-62024-second-report-application-general-data_en).

[32] P. de Hert et al., *EU cross-regime enforcement, redundancy and interdependence. Addressing overlap of enforcement structures in the digital sphere after Meta*, Technology and Regulation, 2024.

[33] EU Parliament, *Newly proposed GDPR procedural rules: Improving efficiency and consistency*, 2024 (https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/757612/EPRS_BRI(2024)757612_EN.pdf). See also H. MILDEBRATH, EPRS - European Parliamentary Research Service, *An analysis of the newly proposed rules to*

in order to allow the Union to achieve the uniformity of application that is necessary and which cannot be postponed).

All these problems, summarized for brevity under the expression "multi-level enforcement concerns", can produce (and do produce, as we shall see) different models of regulatory enforcement, imposing on jurists and interpreters some relevant considerations regarding the effectiveness of such an approach (*infra*).

In conclusion, *multi-regulatory concerns* and *multi-level enforcement concerns* represent two macro-areas of criticality in the European approach to the digital and must be addressed organically.

The diagnosis is clear: the multi-level nature of enforcement, which should be the strong point of the European legal order (capable of bringing the guarantee of rights closer to individuals), risks turning into a "polycentric irresponsibility", in which no institutional actor is clearly accountable for systemic incoherencies. The multiplication of authorities, coordination fora, networks, boards and offices corresponds neither to a functional specialization nor to a clear allocation of ultimate responsibility. In this sense, the new GDPR Procedural Regulation[34] – by harmonizing timelines, procedural guarantees and cooperation mechanisms in cross-border cases – can be read as the first, partial reaction to this drift: it acknowledges that without effective and uniform enforcement, the celebrated "Brussels Effect" risks to remain a rhetorical formula. Yet, similar efforts are still lacking for AI, data and platform regulation, where the same logic of concurrent competences and intersecting mandates is replicated without a coherent "constitutional" design of digital enforcement.

2. Why Now

To achieve a truly competitive European digital regulatory ecosystem, the knots must be untied now: the Commission itself, in the State of the Digital Decade 2025, records "fragmented markets" and "excessively complex regulations", indicating that this slows innovation and scale-up and requires urgent action. Not only that: as recently highlighted by the Court of Auditors, the EU shows poor results in developing a European AI ecosystem (failing to accelerate investment in the sector at a pace comparable to competitors;[35] all the more while these appear to be moving in the opposite direction, as evidenced by President Trump's recent revocation of the Biden administration's Executive Order on responsible AI development,[36] in addition to the recent "AI Action Plan" issued by the White House, which indeed lists the promotion of innovation and adoption among its key points[37]).

The urgency of reform is no longer merely theoretical. The Commission's 2025 Work Programme has formally withdrawn the ePrivacy Regulation proposal, signaling a shift from regulatory accretion to

strengthen GDPR enforcement in cross-border cases, 2024, who highlights some of the shortcomings of the reform proposals.

[34] See https://www.europarl.europa.eu/legislative-train/theme-protecting-our-democracy-upholding-our-values/file-specifying-procedural-rules-relating-to-the-enforcement-of-the-gdpr.

[35] EU Court of Auditors, *Stronger governance and increased, more focused investment essential going forward*, 2024 (https://www.eca.europa.eu/ECAPublications/SR-2024-08/SR-2024-08_EN.pdf).

[36] C. CATH, S. WATCHER, B. MITTELSTADT et al., *Artificial intelligence and the "Good Society": the US, EU and UK approach*, in *Science and Engineering Ethics*, 2018.

[37] https://www.whitehouse.gov/articles/2025/07/white-house-unveils-americas-ai-action-plan/. It is worth remembering that President Trump also expressed criticism of copyright regulations in AI, pointing out that "it is unrealistic" to expect AI programs to pay for every piece of content used during training.

simplification in the digital *acquis*. At the same time, Europe's AI investment and adoption gap relative to the United States is well-documented by Stanford HAI[38] and the EIB, underscoring how legal certainty and lower compliance friction are now competitiveness variables.[39] Against the Digital Decade target of 80% basic digital skills by 2030, the Union stands at 55.6% in 2025,[40] making progress fragile unless rule-sets are better aligned across privacy, content, competition and cybersecurity. In parallel, the Council and the European Parliament have just agreed on how to make cross-border GDPR[41] enforcement faster and more coherent: an intervention that *de facto* acknowledges the need to strengthen enforcement before the over-production of norms generates further compliance costs and uncertainty.

Moreover, part of the scientific literature[42] indicates that, in AI, the "Brussels effect" could manifest only in part or with ambivalent outcomes, considering the structure of the sector and the nature of the AI Act, offering a caution to focus on implementation and competitiveness at least as much as on norm-making. Absent simplification, the digital rulebook risks "heterogenesis of ends" in the Mertonian sense: well-intentioned instruments producing negative unintended effects on innovation and the single market, as echoed in latest OECD analyses.

There are also reasons of legislative economy: the Commission has recently launched Omnibus simplification packages[43] to reduce administrative burdens and improve the European economic ecosystem (indicating simplification as a priority of the European agenda for 2025),[44] while the public debate has even seen requests to "stop the clock" on the AI Act (which Brussels nevertheless rejected): converging signs that attention is shifting from producing new rules to rationalizing those already in force.

In short, the combination of regulatory complexity, application criticalities, and global competitive pressure argues for intervening now (with urgency) on simplification and enforcement, to avoid replicating with the AI Act the weaknesses that emerged in the application of the GDPR.

The "why now" thus has a constitutional, not only economic, justification. A legal order that builds its international influence on regulatory power cannot afford a growing gap between proclaimed leadership and empirical capacity to attract investment, talent and technological infrastructures. The Draghi Report explicitly links competitiveness to the reduction of regulatory uncertainty and to the completion of the Single Market; the Letta Report denounces the stratification of sectoral regimes and national exceptions as a factor of internal dis-integration. If the EU does not realign its digital rulebook with its own constitutional principles of proportionality, loyal cooperation and sincere coordination, the risk is twofold: de

[38] In 2024, U.S.-based institutions produced 40 notable AI models, significantly outpacing China's 15 and Europe's three (https://hai.stanford.edu/ai-index/2025-ai-index-report).

[39] According to the European Investment Bank Group, as stated by the Investment Report 2024/2025, "*there are three key drivers to consolidate Europe as a global leader in new technologies: market integration, simplification and* [the need for] *large-scale investment in innovation"* (https://www.eib.org/attachments/lucalli/20240354_investment_report_2024_en.pdf).

[40] https://digital-strategy.ec.europa.eu/en/policies/2025-state-digital-decade-package.

[41] https://www.consilium.europa.eu/en/press/press-releases/2025/06/16/data-protection-council-and-european-parliament-reach-deal-to-make-cross-border-gdpr-enforcement-work-better-for-citizens/.

[42] M. ALMADA, A. RADU, *The Brussels Side-Effect: How the AI Act Can Reduce the Global Reach of EU Policy*, in *German Law Journal*, published online by Cambridge University Press, 2024.

[43] https://single-market-economy.ec.europa.eu/publications/omnibus-iv_en.

[44] https://commission.europa.eu/law/law-making-process/better-regulation/simplification-and-implementation/simplification_en.

facto de-europeanisation of innovation chains (relocation, forum shopping, reliance on non-EU infrastructures) and internal delegitimisation of the European regulatory project, perceived as a sophisticated source of vetoes rather than as an enabler of freedoms and opportunities. Hence the need for a shift from the quantitative paradigm (more rules, more protection) to a qualitative paradigm (better rules, integrated enforcement, explicit balancing among rights and public interests).

3. Regulatory Overlap: Some Representative Examples

As is well known, the ePrivacy Directive and the GDPR have – *rectius*: would have – different scopes, since only the latter would be intended to protect (only) personal data. It is equally well known, however, that since the arrival of the GDPR risks of normative overlap between the two sources have been highlighted (so much so that as early as January 2017 the Commission approved the draft ePrivacy Regulation, reforming the Directive, with the aim – later specified[45] – of "adapt[ing] the e-Privacy rules to the new technological reality, and align[ing] them to the 2016 General Data Protection Regulation"). The ePrivacy Regulation aimed to introduce a coherent EU-level regulatory framework that would have expanded data protection, clarified consent to cookie use, and defined the scope of covered organizations. However, the proposal was recently withdrawn in February 2025, without an explicit substitute.[46] The withdrawal highlights the intrinsic difficulties of the Union's law-making process and, at the same time, makes an organic reform of the matter even more urgent (even more so given that this is a rapidly evolving field, for which a ten-to-fifteen-year-old regulatory framework appears dated).

A few examples of regulatory overlap affecting the GDPR suffice:

I: between the GDPR and the ePrivacy Directive, on cookies and consent: on the one hand, the GDPR's consent – and other legal bases for processing – which apply generally (Articles 4(11), 6, 7, and 95 GDPR, and Recital 173 GDPR), on the other, the well-known Article5(3) of the Directive. This has always been a particularly debated point, as evidenced by EDPB Opinion 5/2019,[47] the "Guidelines 2/2023 on Technical Scope of Article 5(3)of the ePrivacy Directive" adopted on October 7, 2024, or the "Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR" (for which "under the ePrivacy Directive, the sending of unsolicited communications for purposes of direct marketing… can only take place with the prior consent… to be obtained should meet the requirements set out in Article 4(11) GDPR". Shortly thereafter it is also specified that "It should be noted that Article 5(3) ePrivacy Directive also requires consent for the use of tracking techniques, such as storing cookies or gaining access to information in the terminal equipment of the user. Therefore, when these techniques are used in the context of direct marketing

[45] EU Parliament, Briefing - EU Legislation in *Progress*, *Reform of the e-Privacy Directive*, Sept. 2017, 2.

[46] Among the reasons given is "No foreseeable agreement – no agreement is expected from the co-legislators. Furthermore, the proposal is outdated in view of some recent legislation in both the technological and legislative landscape" (which highlights, among other things, another critical issue in the European regulatory process: the excessive complexity of the legislative process, ed.). In *The European Commission Withdraws the ePrivacy Regulation*, Feb. 2025, 27-29 (https://commission.europa.eu/document/download/7617998c-86e6-4a74-b33c-249e8a7938cd_en?filename=COM_2025_45_1_annexes_EN.pdf).

[47] EDPB, *Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR in particular regarding the competence, tasks and powers of data protection authorities*, 2019 (https://www.edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf)

activities, such consent requirements under Article 5(3) ePrivacy Directive must be respected…[while] any processing operations of personal data following the aforementioned processing operations, including processing personal data obtained by accessing information in the terminal equipment, must have a legal basis under Article 6(1) GDPR to be lawful… thus normally precluding reliance on Article 6(1)(f) in this context"). Those acts, while certainly pursuing legal clarity, often remain excessively generic and hard to interpret: the same Guidelines specify that direct electronic marketing operations *may* fall under both frameworks, or only within the Directive's scope, or only under the GDPR, *depending* on the types of data processed, and that in *any* case controllers *should* also assess the scope of national rules transposing the ePrivacy Directive at Member-State level, which *may* occasionally impose consent requirements that go beyond those laid down in the Directive. Is it really possible to expect that individual digital operators can extricate themselves from this interpretive labyrinth? The excessive complexity of the matter seems to be confirmed by the recent large-scale sanctions imposed by the CNIL on some providers,[48] under Article 82 of the French Data Protection Act, for violations – note well – of its own guidelines and recommendations.[49] And if these large actors struggle, what of smaller entities, which certainly cannot count on in-house departments devoted solely to compliance? All the more so as the picture becomes even more complex when it comes to establishing minimum thresholds of protection (as with the work of the Cookie Banner Taskforce, whose positions however "have to be combined with the application of additional national requirements stemming from the national laws transposing the ePrivacy Directive in the Member States, as well as to further clarifications and guidance provided by the national competent authorities to enforce the law transposing the ePrivacy Directive at national level, which remain fully applicable"),[50] or when particular interests come into play, such as those of minors (see Article 28 of the Digital Services Act, indicated by Commission spokesperson Thomas Regnier as a framework that protects citizens' privacy).[51]

II: between the GDPR and the rules on cybersecurity and AI, in the event of a data breach: as it is well known, most data breaches today are represented by cyber-attacks, and thus by cybersecurity violations. As expressly indicated by the "Guidelines 9/2022 on personal data breach notification under GDPR" (version 2.0 of 28 March 2023), "although the NIS Directive requires competent authorities and supervisory authorities to cooperate and exchange information in this context, the fact remains that, where such incidents constitute or become personal data breaches within the meaning of the GDPR, such operators and/or providers would be required to notify the supervisory authority separately from the incident notification obligations under the NIS Directive",[52] since the GDPR has rendered notification obligations

[48] CNIL, *Cookie regulation: the CNIL is continuing the action plan initiated in 2019 and has imposed two fines on SHEIN and GOOGLE* (https://www.cnil.fr/en/cookie-regulation-cnil-continuing-action-plan-initiated-2019-and-has-imposed-two-fines-shein-and#:~:text=SHEIN%20and%20GOOGLE-,Cookie%20regulation%3A%20the%20CNIL%20is%20continuing%20the%20action%20plan%20initiated,fines%20on%20SHEIN%20and%20GOOGLE&text=The%20CNIL%20fined%20GOOGLE%20325,with%20the%20rules%20on%20cookies).

[49] In January 2022, the CNIL had already fined Google (€150 million) and Facebook/Meta (€60 million) for making it difficult to refuse cookies as easily as accepting them.

[50] https://www.edpb.europa.eu/system/files/2023-01/edpb_20230118_report_cookie_banner_taskforce_en.pdf.

[51] https://techcrunch.com/2025/02/12/eu-abandons-eprivacy-reform-as-bloc-shifts-focus-to-competitiveness-and-fostering-data-access-for-ai/.

[52] *Ivi*, 28.

virtually inevitable (unlike under the Data Protection Directive 95/46/EC, replaced by Regulation 2016/679). Nor is different between GDPR and AI Act: considering that the GDPR provides an obligation to report "equivalent" to that laid down by Article 73 of the AI Act, this would logically mean that when a data breach caused by an AI system comes to light, it is likely to entail a risk for the rights and freedoms of natural persons: the data controller should therefore notify the incident also to the national market-surveillance authority under the AI Act, as well as to the national data-protection authority under the GDPR;[53] creating a "notifications overload" for entities falling within the scope of two or more Union laws;
III: between GDPR and AI Act, on risk assessment: it is known that the GDPR's DPIA is required when "new technologies" are used for "high-risk" processing; while the AI Act's FRIA requires that before putting a high-risk AI system into use, the interested entities carry out a fundamental rights impact assessment: it is evident that where the use of an AI system entails the processing of personal data, an overlap can thus arise: both DPIA and FRIA may need to be carried out. It is true that the AI Act expressly coordinates the two requirements, providing for information flows between deployer and provider and providing that the FRIA "completes" the DPIA, but – for example – some obligations will remain duplicative: is it really necessary that public bodies should register a summary of the FRIA and also a summary of the DPIA?[54] Moreover, it is not difficult to imagine conflicts arising – first and foremost interpretive – on the co-existence of the two instruments, or even on being subject to both or only one of them. While it is true that DPIA and FRIA have contiguous but distinct purposes and legal rationales, it is undeniable that normative overlap – when a high-risk AI system also involves personal data – is highly likely.
Such complexity creates legal uncertainty for digital business models, cross-border data flows and undermines the objectives of the Digital Single Market (put in a more economic perspective: disproportionate and unbalanced interpretations of key concepts constitute a great barrier to innovation and investment due to a culture of risk aversiveness – zero risk being the preferred default for regulators).
And again, further examples can be given also for the (forthcoming) application of the AI Act:
A: beyond what has already been said in relation to DPIA–FRIA, risk-assessment operations may in fact be required both under the AI Act and under the Digital Services Act: although for different purposes and with different aims, both frameworks require risk analyses and can therefore oblige addressees to perform this operation with different cadences or modalities, duplicating the efforts and burdens required for compliance;
B: the same can happen also for content labelling: the AI Act seems to require platforms to label as AI-generated the content generated by their own AI tools, while the DSA can potentially require them to label likewise content generated by third-party AI, generating uncertainty;[55]
C: even more evident is the possible overlap between AI Act and MDR,[56] which could create a significant regulatory burden, with predictable interpretive difficulties and slowdowns, easily forecastable for the

[53] T. KARATHANASIS, *AI incident notification in the Eu Ai Act: how does it work and is it effective?*, in *AI-Regulation Papers*, 2024, 8.
[54] EU Reg. 2024/1689, Annex VIII, Section C, points 4–5.
[55] A recent article published on DSA Observatory (P. LEERSSEN, *Embedded GenAI on Social Media: Platform Law Meets AI law*, in *DSA Observatory*, 2024) highlights that "Social media platforms are integrating generative AI features into their services", con "features [that] trigger overlapping obligations under the AI Act and the Digital Services Act".
[56] While the MDR identifies four risk classes for medical devices, from low to high, based on a series of criteria (e.g., invasiveness, duration of use, part of the body involved, etc.), Article 6 of the AI Act seems to disregard such an

development and marketing times of new technologies, further jeopardising the competitiveness of the European MedTech sector and its consumers;[57] or the potential conflict between transparency and competition: while numerous provisions of the AI Act (Articles 19; 16, 23, 24, 25) require the sharing of technical documentation[58] and training data, it is evident that this could entail the dissemination of industrial data and damage competition on the market.[59]

One could go on (also by highlighting the repercussions – for example – of over-regulation on competition, or on civil liability,[60] or for the financial sector).[61] The picture described shows particularly high non-compliance costs, high multi-authority application complexity (hundreds of cross-border cases per year, with a portion requiring binding decisions), often in areas where regimes overlap (cookies, security/breach),[62] and ever-greater interpretive difficulty (with consequent resource expenditure for economic operators wishing to operate in the European market).

The impacts of over-regulation and regulatory overlaps concentrate where the most significant economic volumes and strategic functions flow. The platforms/tech ecosystem directly affects digital revenues, with around 96.9 billion euros in online advertising spend in Europe in 2023 (harmonized across 29 markets),[63] so regulatory uncertainties translate immediately into compliance costs in VLOPs' business model (and even more for smaller platforms); while European med-tech (worth 160 billion euros in 2023) will reach 170 billion euros in 2024, confirming the systemic weight of overlaps and duplications of compliance on clinical and diagnostic spheres.[64] Not to mention finance (the value added of the "financial and insurance activities" aggregate in the EU is 0.9 trillion euros),[65] or the public-services sector, where the lever of digital procurement weighs around 14% of EU GDP (around 2,000 billion euros/year),[66] so that any overlaps/duplications propagate along the entire chain of suppliers and transformation projects; or the

assessment, identifying the use of AI systems within medical devices subject to third-party assessment as a sufficient criterion. etc.), Article 6 of the AI Act seems to disregard such an assessment, identifying the use of AI systems within medical devices subject to third-party assessment as a sufficient criterion for classifying such AI systems as "high risk" – regardless of whether there is a real risk to human health or safety.

[57] See the 2022 survey by the European association MedTech Europe: of the more than 470 companies surveyed, more than half said they were deprioritizing the European market for the launch of new medical devices medtech-europe-survey-report-analysing-the-availability-of-medical-devices-in-2022-in-connection-to-the-medical-device-regulation-mdr-implementation.pdf.

[58] Not only that: some regulatory provisions are also difficult to apply and risk discouraging the adoption of AI in medicine. One example is the obligation "to provide complete information also concerning the decision-making logic of the computer systems that may be involved in the diagnostic or therapeutic activity (all this bearing in mind the well-know forms of opacity of AI systems)".

[59] A. STAZI, *AI Act, Competition and Fairness. Compliance Issues, Overlaps in EU Legislations and Global Regulatory Scenario*, 2025, 4.

[60] *Ibid*.

[61] DORA explicitly recognizes "gaps or overlaps" in key areas (incident reporting, resilience testing), to be coordinated with horizontal regimes such as NIS2 (see EU Reg. 2022/2554, Recitals 10, 24, 26, and 93).

[62] EDPB, Annual Report 2023, 27.

[63] IAB Europe, https://iabeurope.eu/iab-europe-adex-benchmark-report-2023-reveals-exceptional-strength-and-growth-of-digital-advertising-in-europe/.

[64] MedTech Europe Facts & Figures, 2025 (https://www.medtecheurope.org/wp-content/uploads/2025/09/medtech-europe-facts-and-figures-2025-digital-1.pdf).

[65] Eurostat, 2022.

[66] EU Commission, https://single-market-economy.ec.europa.eu/single-market/public-procurement_en.

cloud/data-sharing market: 45.2% of EU enterprises purchased cloud services in 2023, showing the pervasiveness of data infrastructures, while the EU-27 Data Market is worth 90.0 billion euros in 2024, with regulatory overlaps impacting – at every level – value chains in every sector.[67]

Moreover, beyond the points made above, it is worth recalling that EU regulatory framework features not only regulatory overlaps but also traces of regulatory overreach (that is, cases in which the law exceeds its intended purposes, with harmful effects on the enforcement ecosystem).

This can be seen, for example, as for the GDPR, in the "pay or consent" model: whereas in Europe – following EDPB Opinion 8/2024 – platforms must offer an "equivalent alternative" to "pay or consent" without behavioural advertising, preferably free of charge; in the UK the ICO appears to have considered that no such obligation is contained in, and thus cannot be derived from, privacy legislation.[68]

The same happens with the AI Act: the Commission's 2021 draft was built to regulate uses of AI systems via a risk taxonomy, and the GPAI systems weren't in that blueprint: they entered the file only with the Council's general approach and the 2023 trilogue deal. This late grafting explains some conceptual strain and implementation fragility: article 51 AI Act now presumes that a GPAI model has "high-impact capabilities" (and thus systemic risk) if training compute exceeds 10^25 FLOPs, directly conflating model size measured in FLOPs with the existence of a "systemic risk" and thus introducing a presumption on the technology itself (and *not on its usage*, as the AI Act should be intended to do: it must be underscored that AI regulation never intended to regulate the technology in and of itself – least of all by assuming it to be *a priori* risky – but only to regulate uses of the technology, in particular those uses that constitute a risk to fundamental rights and freedoms). At the same time, the Regulation seems to require assurances from providers that, however, will not always appear possible;[69] while "guidance-after-obligations" concerns are arising (GPAI rules started applying August 2nd, 2025, yet the Code of Practice and interpretive Guidelines for GPAI landed only in July 2025, compressing implementation windows. In parallel, CEN-CENELEC warned that several harmonised standards will slip into 2026, so firms face hard obligations before stable technical norms exist).[70]

---

[67] EU Commission, *Cloud computing – statistics on the use by enterprises*, 2025 (https://ec.europa.eu/eurostat/statistics-explained/SEPDF/cache/37043.pdf).

[68] See M. BARCZENTEWICZ, *Why is Meta offering cheaper and simpler 'pay or consent' in the UK?*, EUTechReg, 2025, which further highlights that several studies find users exhibit a low willingness to pay for privacy.

[69] It has been highlighted that "The Commission's original proposal focused on a risk-based approach to deploying AI systems, assuming a value chain that divided responsibilities between providers of AI systems (or models), and deployers, importers and distributors of these systems. In trilogues, law-makers insisted on the final Act including a specific regime dealing with general-purpose AI models – influenced heavily by the just-announced released of ChatGPT. This new regime creates conceptual complexity in the Act, with unanswered questions about the correct allocation of responsibilities across the AI value chain. It has also led to the law including presumptions about how the AI value chain works, which may not always prove realistic in practice and have been challenged by emerging models like DeepSeek. For example, the law seems to assume that general-purpose AI models will serve as inputs for specific AI applications, and that significant responsibility could be put onto the providers of these models. In practice however, today, many general-purpose AI models are learning from each other – such as by models using other models' outputs as their own training data– meaning in practice a model provider may not be in a position to provide the assurances the AI Act requires, particularly where open-source AI models are involved since these are subject to fewer regulatory obligations in some cases"…making "unclear whether the law is particularly well designed for this market development". (Z. Meyers, *op. cit*.).

[70] Euronews (C. KROET), *EU standards bodies flag delays to work on AI Act*, 2025.

It is evident that in some sectors – more than in others – there is an urgent need for greater simplification. We can conclude that these sectors are privacy (in particular, collection and management of consent; direct marketing); competition (in particular, the balance among privacy, innovation and economic growth); AI (in particular, the copyright regime, risk-calculation models, cross-border cases); cybersecurity (in particular, notification obligations).

4. The Charter of Fundamental Rights of the EU: A Possible Interpretive Key?

It must be recalled that privacy and data protection are fundamental rights enshrined in EU primary and secondary law. Article 7 of the Charter of Fundamental Rights of the Union enshrines the right to privacy, stating that "everyone has the right to respect for his or her private and family life, home and communications". Article 8 of the European Convention on Human Rights likewise enshrines the right to privacy. Pursuant to Article 52(3) of the Charter of Fundamental Rights of the Union, the meaning and scope of the fundamental rights guaranteed by the Charter must be interpreted in the same way as the ECHR. The protection of natural persons with regard to the processing of their personal data is also a fundamental right, enshrined in Article 8 of the Charter.[71] Article 8 of the Charter furthermore provides that personal data "must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law". The main current instrument for data and privacy protection in EU secondary legislation was the Data Protection Directive (95/46/EC), complemented, as regards the confidentiality of electronic communications, by Directive 2002/58/EC (the e-Privacy Directive). The GDPR then replaced the 1995 Data Protection Directive with general principles and rules to be applied when private- or public-sector entities process personal data (for example, conditions for lawful processing, obligations and rights arising from processing, and safeguards); whereas the e-Privacy Directive aims to avoid unjustified restrictions on the free movement of data, considered essential for innovation and competitiveness. Consequently, the processing of personal data is permitted under certain conditions, provided that data subjects retain their right to privacy, freedom of expression, and other rights. An approach, in short, based on rights and closely correlated with self-determination and human dignity (as enshrined in Article 2 of the Charter of Fundamental Rights of the European Union).

In light of this, it is possible to affirm that the EU Charter of Fundamental Rights should orient more forcefully the application and conception of technology regulation (GDPR, e-Privacy Directive and related acts), because the balancing among privacy/data protection (arts. 7–8), freedom of expression and information (art. 11) and freedom to conduct a business (art. 16) is required by the very architecture of the Charter, according to the criteria of necessity and proportionality in art. 52(1). In positive law, the GDPR makes explicit that data protection is not an absolute right and "must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality": for this reason the legislation links such balancing to the need for trust to enable the development of the digital economy in the internal market (Recitals 4 and 7), for the creation of a regulatory ecosystem that transcends the mere "privacy" dimension as an end in itself. The balancing operation is not an ethical aspiration but a constitutional rule: art. 52(1) of the Charter binds the legislator and the enforcement

[71] For these and subsequent considerations, see European Parliamentary Research Service (S. MONTELEONE), *Reform of the e-Privacy Directive*, 2017.

authorities to limit rights only if provided by law, in respect of their essence, and with measures necessary and proportionate to objectives of general interest or to the protection of the rights of others, and this includes equally Arts. 7–8 and Arts. 11 and 16, which recognize the centrality of the circulation of information and of economic initiative in contemporary digital ecosystems.

According to the case-law of the European Court of Human Rights, the protection of personal data is a fundamental component of the right to private life. Similarly, the case-law of the Court of Justice has thus far set the center of gravity firmly on the rights in Articles 7-8 in matters such as data retention and access. In *Digital Rights Ireland*[72] and then in *Tele2 Sverige/Watson,*[73] the Court invalidated generalized data-retention schemes for violation of the rights to private life and to data protection, referring to the standard in Art. 52(1): this confirms that the balancing is real but starts, for historical reasons, from a reinforced protection of the private sphere (as already seen also in the *Schrems* cases). In *La Quadrature du Net,*[74] the Grand Chamber reiterated the strict limits on generalized retention or on real-time access to traffic/location data, stressing that any derogations must respect the test of necessity and proportionality in light of Articles 7-8-11 and art. 52(1); once again the hard core of privacy acts as a counterweight, but the textual reference to art. 11 signals the existence of a polycentrism of rights online. On the other hand, the balancing was already present, on closer inspection, in the very first case that would then give rise to one of the GDPR's founding principles: in *Google Spain*, the Court of Justice balanced the protection of the person with the public's interest in information and freedom of expression, showing that the outcomes depend on contextual evaluations (rather than relying on pro-privacy automatisms).

Given this background, the Charter has to be understood *pro futuro* not only as dogmatic confirmation of the centrality of privacy and data protection, but as an operational criterion for interpreting the entire body of digital regulation. A Charter-consistent reading of the EU digital framework requires regulators and Courts to justify how restrictions on data processing, obligations on providers, or limitations on automated decision-making respect the essence of the affected rights and satisfy the proportionality test in light of all the interests at stake. In practical terms, this implies that guidelines, opinions and soft-law instruments issued by data protection Authorities, digital services coordinators etc. should explicitly articulate the balancing between articles 7–8 and articles 11 and 16 CFR, rather than silently presuming the structural prevalence of one dimension. Where several equally rights-compliant interpretations are available, preference should be given to those that enable, rather than obstruct, the deployment of privacy-enhancing technologies, data protection by design solutions and secure data re-use serving research, innovation and democratic scrutiny.

In other words, th EU need an applied language that makes the balancing explicit and does not end in compliance checklists, and that is capable of understanding when one can (or cannot) speak of a violation of the essence of the right (whose "interferences […] need to be examined within the framework of the principle of proportionality"):[75] read in this light, the Charter offers the missing normative compass for navigating the crowded field of EU digital regulation: it prevents the emergence of a purely data-centric

[72] C-293/12 e C-594/12 (joined cases).
[73] C-203/15.
[74] C-511/18.
[75] M. Brkan, *The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning*, in *German Law Journal*, *Cambridge University Press*, 2019, 882.

monism and anchors the interpretation of overlapping regimes to a common set of principles capable of reconciling individual rights, democratic values and the enabling conditions for innovation.
In this perspective, innovation is not an antagonist of rights, but a means of development (for example, the use of privacy-enhancing technologies – such as differential privacy but not only – enables analysis, sharing and re-use while reducing exposure and risk, as shown by ENISA's work on data spaces and OECD syntheses that connect PETs to industrial and research use-cases).[76]
Innovation and compliance are not adversaries, but integrate: this increasingly appears to be a reading of the European regulatory framework consistent with the principle of proportionality and with the mandate of the GDPR. In terms of method, this means motivating enforcement decisions and guidelines not only with the language of minimization and security, but by making transparent the balancing among rights (including articles 11 and 16) and indicating, when available, less restrictive technical alternatives that equivalently achieve the protection objectives, according to art. 52(1) (a repositioning that is, in reality, already inscribed in the text of the sources: the Charter requires proportionality and respect for the essence of rights; the GDPR requires trust and the development of the information society, without consecrating *a priori* hierarchies).
In conclusion, one cannot fail to see that a systemic analysis of the technological framework, consistent with the Charter, must abandon a monistic and "data-centric" interpretation and assume – also in the public discourse (and in soft-law instruments, and not only; *infra*) – that the balancing among privacy, expression and enterprise is prescribed by Union law and is facilitated by technological innovation when this is thought by design, according to the "state of the art", to realize the proportionality required by art. 52(1).

5. Towards a Multi-Level Economic Constitutionalism

The notion of a multi-level economic constitutionalism provides an appropriate lens through which to read the European Union's attempt to govern the digital economy. The shift from a state-centred paradigm to a system in which regulatory authority is shared between the Union, the Member States and a dense network of independent authorities has already impacted on European economic governance.[77] In the digital field, this structure intersects with the presence of global private actors whose infrastructural power conditions access to markets and to the public sphere. The result is an environment in which constitutional questions concerning competences, guarantees and accountability can no longer be posed solely in vertical, public-law terms, but must take into account the triangular relationship between EU institutions, Member States and large platforms or service providers.[78]

[76] OECD (https://www.oecd.org/en/publications/emerging-privacy-enhancing-technologies_bf121be4-en.html); see also ENISA, *Engineering Personal Data Protection in EU Data Spaces*, 2024.
[77] See also E. C. RAFFIOTTA, *The Twenty-First Century Economy Between Global Law and National Legal Systems: The Strength of the Market and the Weakness of the State*, in *Democratic Protests and New Forms of Collective Action. When Disobedience is Social* (LM Daher, ed.), Springer, 2023.
[78] M. BARONI, *Costituzione polemica. Orientarsi nello stato di crisi permanente per riscoprire la dignità e l'autorealizzazione individuale* (II ed.), Editoriale Scientifica, 2024, writes of "constitutional tendencies" of large private platforms.

Within this configuration, the dense body of rules on data, platforms, artificial intelligence and cybersecurity is clearly the normative expression of a European choice to constitutionalise the digital economy: by binding both public and private actors to fundamental rights standards, competition principles and procedural safeguards, the Union projects its constitutional identity into the market. Yet, as the analysis of multi-regulatory and multi-level enforcement concerns has shown, this process is exposed to the risk of heterogenies of ends. Regulatory layering overlaps among regimes and fragmented enforcement can inadvertently favor the most structured global players, who are able to absorb compliance costs and navigate complexity, while discouraging smaller European operators and public entities. In such a scenario, the digital single market risks remaining formally integrated but materially segmented, with innovation and data-driven services relocating outside the Union.[79]

To prevent this outcome, multi-level economic constitutionalism must be given concrete operational content. The interaction between competition law, sectoral regulation and fundamental rights could be better framed within a coherent constitutional narrative: obligations to share data, to ensure interoperability or to refrain from certain forms of profiling and amplification are legitimate to the extent that they are justified as proportionate means to reconcile economic freedoms with the protection of users' rights and with pluralism in digital markets.

A genuinely constitutional reading of the digital single market also requires the Union to treat regulatory coherence, simplicity and legal certainty as components of competitiveness, not as concessions to deregulation. The recent reports on the future of the Single Market and on European competitiveness have underscored how complexity, duplication of procedures and uncertainty regarding competent authorities represent structural obstacles to investment and scale-up. In a multi-level economic constitution, the allocation of regulatory tasks between Union and national levels, and among specialised authorities, must therefore be guided by functional criteria and accompanied by clear coordination mechanisms. Uniform guidance on the articulation between GDPR, DSA/DMA, Data Act, NIS2 and AI Act, joint enforcement teams for systemic cases, and enhanced judicial review of key interpretative decisions would convert the current patchwork into a more predictable and attractive legal environment.

Furthermore, the external projection of the so-called Brussels Effect depends on the internal credibility of this multi-level constitutional framework. In AI governance, numerous international frameworks (as the ones by OECD, G7, UN, EU) set principles but, being largely non-binding, they produce fragmented compliance and uneven enforcement; while divergent approaches (the EU's strict risk-based approach versus more flexible US/China models) deepen the worldwide split. The priority is to coordinate the multi-level EU constitutionalism (public powers) with the EU economic needs and vocation (private powers), in order to achieve concrete enforcement, cross-border coordination, and legally enforceable standards. In fact, the Union can expect third countries and global firms to adapt to its digital standards only if it demonstrates, domestically, that those standards are enforceable, proportionate and compatible with innovation. Otherwise, there is a risk that the European model will be perceived as normatively ambitious but economically dissuasive, encouraging forum shopping and technological dependence on non-EU infrastructures; while a constitutionalized digital economy, by contrast, would combine high levels of rights

[79] See also G. Noci, *Disordine. Le nuove coordinate del mondo*, in *Il Sole 24 Ore*, 2025, for a broad vision about the inner complexity of the XXI economic and societal scenario.

protection with clear and streamlined compliance pathways, thereby transforming the density of EU law into a competitive advantage for operating within a large, integrated and rights-based market.
Finally, in that perspective we cannot ignore the material preconditions for its own effectiveness: if regulatory choices presuppose significant investments in security-by-design, explainability, monitoring and enforcement, the Union must ensure that public funding, industrial policy instruments and capacity-building strategies are aligned with these requirements. Otherwise, sophisticated regulatory frameworks risk producing a dual regime in which only major players fully comply and influence the interpretation of the rules, while smaller actors are pushed to the margins of the European digital space. Embedding questions of distribution and access to resources within the constitutional analysis of the digital single market is indispensable to avoid a gap between the formal universality of the Charter and the selective material enjoyment of digital rights and opportunities.
In this sense, the language of multi-level economic constitutionalism highlights the conditions for articulating a European strategy in which digital sovereignty, market integration and fundamental rights mutually reinforce each other. Only by consciously designing the relationship between levels of governance, sources of law and categories of actors can the Union prevent regulatory fragmentation and over-production from undermining its own objectives, and instead turn its constitutional commitments into a tangible asset for citizens, administrations and undertakings operating in Europe's digital environment.

5.1. *Quid Iuris?* Some Normative Reform Proposals

Considering what has been described above, it is clear that the Union's approach to the digital phenomena cannot ignore some necessary changes. Indeed, such changes seem necessary to render regulation truly effective and efficacious, making it capable of keeping pace with inevitable technological change. Otherwise, the concrete risk is to "fall behind" and thus to nullify the human-centered inspiration of the European regulatory framework.
The first changes must be, as it is logical, to intervene directly in the sources that govern the digital phenomena.
Without any claim to exhaustiveness, a few examples can be offered.
With regard to data protection, it must be noted that the word "innovation" still never appears expressly in the text of the GDPR: the text should be reformed so that the necessary balancing between the protection and safeguarding of rights on the one hand, and technological innovation on the other, is clear (as noted, an approach that fails to take the latter into account will inevitably end up nullifying both). The same can be said for "economic growth": that expression too does not appear in the legal text, even though it is famously identified as one of the pillars of the Union.
Again, reform of the GDPR's founding principles should provide the occasion for the necessary and no-longer-postponable reference to a renewed balancing that takes account of fundamental rights: as constitutional experience teaches, balancing cannot be understood as an operation governed by absolute rules but must instead be assessed case by case. Any *a priori* classification will always prove incapable of including the cases of everyday experience, inevitably resulting in ineffectiveness: one solution could be to place greater responsibility on providers and platforms, providing for forms of *ex post* control of the balancing. After all, such a structure appears consistent with the controller's accountability principle.

Definitions used in European regulation should then be simplified and harmonized: the recent proposals to reform the GDPR envisage a change to the definition of small and medium-sized enterprises (broadening its scope) but provide nothing on harmonizing that definitional change with other Union rules (for example, the NIS2 Directive does not draw, in numerous sectors, any categorical distinction).

The harmonization of the rules must also operate prospectively. Consider the case of the need to respect the minimization principle under the GDPR, on the one hand, and the need to employ large (and high-quality) datasets to train AI systems – which is necessary to avoid bias and "hallucinations" – on the other. Exemptions should therefore be envisaged from the application of some rules that may conflict with one another, providing for an *ex ante* justification system.

Nor does it seem possible to postpone any further reform of the ePrivacy Directive, now belonging to a time that is excessively remote and out-dated: the EDPS itself, it should be recalled, had issued an opinion calling for rules that are "smarter, clearer and stronger".[80] In particular, there are some evident problems with the Directive, including limited transparency regarding cookies used for tracking and shortcomings in the method commonly used to request consent through "take it or leave it" banners or "cookie walls" (Article 5(3) of the e-Privacy Directive); or the scope of the provision in Article 5(3) (confidentiality of communications) which has been considered both too broad (it should not include first-party analytics) and too narrow (it should consist of all tracking techniques). REFIT's own evaluation indicated that the consent rule is superabundant (as it also covers practices not detrimental to private life) and its implementation can prove challenging for businesses.

The aforementioned simultaneous application of GDPR and the ePrivacy Directive to cookies and consent, as well as overlapping requirements between the GDPR, DSA, DMA, and the Data Act, represent undeniable yet problematic examples of regulatory overlaps: which the EU could counteract by considering mechanisms such as regular regulatory reviews and sunset clauses to prevent future overregulation and ensure ongoing coherence.

A more equitable balancing must then be found between users' rights and industry interests (in line with the balancing required by the Charter of Fundamental Rights, as described above, Articles 7 *et seq*.). The draft Regulation to reform ePrivacy seemed to be moving in the right direction. But even today, some principles of European regulation do not find full application; such as the principle of technological neutrality: the legislator should instead make greater use of technology-neutral definitions, to encompass new technologies and services and to ensure that regulation is suitable for future needs: that need is not by chance expressed also in the UNIDROIT Principles on Digital Assets and Private Law[81] and by the European Law Institute (2022), which in "Principle 3" essentially indicated how the rule must be adapted to the specific characteristics of each technology or product (and not vice versa).[82] Adapting regulation to particular technological solutions would enable the legislator not to be overwhelmed by technological advances, giving it the opportunity to provide exceptions from the original text of the Directive (for example, through pseudonymisation techniques – in line with CJEU C-413/23 P – and PETs).

[80] EDPS, Opinion 6/2017 (https://www.edps.europa.eu/sites/default/files/publication/17-04-24_eprivacy_en.pdf).

[81] UNIDROIT, https://www.unidroit.org/wp-content/uploads/2024/01/Principles-on-Digital-Assets-and-Private-Law-linked-1.pdf.

[82] Critical of the AI Act's lack of complete neutrality, for example, Z. MEYERS, *Better Regulation and the EU's Artificial Intelligence Act*, in *Intereconomics*, 2025, 151.

Finally, simplification is needed. Starting with the consent rule for the use of markers and other identifiers (for example, no consent is necessary for non-privacy-intrusive cookies that improve the user's browsing experience). Or, as noted, by harmonizing application of the Directive with the GDPR, preferring the latter as the general rule on data protection (for example, in cases of overlap between Article 5(3) and the GDPR's legal bases); and finally by repealing security rules that cause regulatory duplication.

The ensemble of Union regulations on the digital phenomenon constitutes a unitary ecosystem, in which the different rules and provisions influence each other. For this reason, if we want a more agile and effective Union, capable of engaging with its competitors as an equal (and with the same speed), discussion of data protection must be accompanied by that on AI. While it is true that the AI Act is still a young regulation, it is equally true that some of its provisions risk becoming obsolete too quickly (indeed, they risk presenting as already obsolete).[83] This is the case of the provisions on GPAI systems, which in fact – as previously seen – were not envisaged in the initial Proposal and which – added later – immediately appeared anachronistic and incapable of keeping pace with technological evolution: an archetypal pathway of regulatory overreach to regulatory obsolescence on arrival.

In order not to betray the Regulation's original spirit, and in order not to render the legal text obsolete from the outset, the AI Act must therefore be made truly capable of following the field's very rapid technological progress: for example, inter-category movements should be envisaged (allowing a technology to be "downgraded" in risk if new safety solutions are provided). In general, automatic application metrics for measuring risk must be eliminated. The output of the Framework Convention of the two Committees established within the Council of Europe, CAHAI and CAI, is helpful in this regard: whereas the FRIA is preventive, the impact assessment under Art. 16 of the Convention moves in both directions (*ex ante* and *ex post*)[84] and, above all, steps out of the AI Act's abstract and general dimension, instead taking account of the context of deployment of the technology and the specificities of use of the AI system: it creates a case-by-case impact assessment (consistent with Recital 5 of the Regulation), which knows neither rigid applications nor presumptions applicable to any AI system irrespective of the specific sector of use.

Furthermore, today's rules penalize European companies. For example in copyright: the interaction between the AI Act and the text-and-data-mining (TDM) exceptions in the CDSM Directive envisages an extraterritoriality clause in Recital 106 of the AI Act: aside from the consideration that this clause is merely contained in a Recital,[85] the clause on extraterritoriality conflicts with the *lex loci protectionis* rule and therefore with the principle of territoriality that governs copyright, as also provided by Regulation (EC) 864/2007, Art. 8. There are therefore issues of legality and, on closer inspection, of enforcement as well: a GPAI model provider will have to comply with both the requirements of Article 4(3) CDSM and the additional requirements of Article 53(1)(c) AI Act. However, it may occur that the party who carried out the

[83] See also F. DONATI, *La protezione dei diritti fondamentali nel Regolamento sull'intelligenza artificiale*, in *Rivista AIC*, 1/2025, according to which the method of identifying the degree of risk of AI systems which, being carried out in the abstract and preventively by the legislator, could prove inadequate in practice or in any case obsolete due to the rapid pace of technological evolution.

[84] See C. NARDOCCI, *Self-Regulation, Regulation e "contro-regolamentazione". Le nuove tendenze: diritto, diritti e intelligenza artificiale*, in *Rivista di Diritti comparati*, 2025, 22.

[85] Which, according to established case law of the CJEU, are not binding – see C-136/04, para. 23; C-134/08, par. 19; or recently M. DEN HEIJER *et al., On the Use and Misuse of Recitals in European Union Law*, in *Amsterdam Law School Research Paper*, 2019.

relevant TDM activity is not a GPAI model provider and is therefore not subject to the AI Act's obligations. In such cases, it becomes difficult to foresee how GPAI model providers can guarantee an effective opt-out for content and datasets prepared upstream by third parties.[86]

What should instead be expanded is the innovative scope of regulatory sandboxes, which – drawing on the experience of financial sandboxes[87] – have proved to be strategic tools for evidence-based regulation, capable of fostering constructive dialogue between regulators and innovators.

Moreover, if it is true that calls to stop the clock for the AI Act have been disregarded, it is nonetheless true that – especially for the most critical provisions – there is still time to change approach. Specifically, it is useful to look in a comparative perspective: for example, by adopting *wait-and-see approaches* (as in South Korea and the United Kingdom),[88] or the ASEAN *light-touch approach*, which eliminates the excessive rigidities of traditional regulation and instead takes account of the specificities of the individual national context.

At the practical level, the Japanese experience is useful, oriented not to a comprehensive regulation of AI (with all the criticalities that may arise, as seen), but to regulation by specific uses, integrated at sectoral level with other existing rules (e.g. in the Personal Information Protection Act—PIPA): a regulatory framework that includes non-binding rules, voluntary corporate guidelines that emphasize risk mitigation and interpretative additions to existing laws, as in the Copyright Act and the Act on the Protection of Personal Information.

The point is important and offers the cue for some considerations on a second line of necessary reforms within the Union.

5.2. *Quid Iuris?* Some Systemic Reform Proposals

The legislative interventions mentioned above are necessary, but they cannot be considered – and of themselves – sufficient if they are not accompanied by a genuine paradigm shift. In particular, the analysis of the Union's rules makes it evidently necessary to direct future activity along two main paths.

On the one hand, institutional simplification can no longer be postponed: overlaps among regulatory sources also cause overlaps among the Authorities competent for the application of those same rules. An initial policy intervention should strengthen the powers of governments (which are usually entitled to appoint these Authorities) by encouraging multi-level dialogue between Member States and the European Union. The lack of coordination between EU policies and Member States (as seen in the application of NIS2) is one of the main obstacles to the effective application of EU law. In this context, it is precisely the expansion of channels for interinstitutional dialogue that will help the EU to establish uniform application

[86] J. P. QUINTAIS, *Copyright, the AI Act, and extraterritoriality*, in *Institute for Information Law* (IViR), 2024, which identifies a possible solution in codes of conduct, to provide incentives for extraterritoriality through market laws. One point can be identified in the AI Act Code of Conduct for general-purpose AI providers, although concerns have already been expressed about its effects (and in particular its feared excessive prescriptiveness). See also P. LAROUCHE, *Legal framework for an effective implementation of the AI Act*, Centre on Regulation in Europe, 2025.

[87] For example, by the Financial Conduct Authority 2017 in the United Kingdom (followed by Spain, also in fintech); or in Italy, Decree Law No. 34 of April 30, 2019; or Germany (https://www.bundeswirtschaftsministerium.de/Redaktion/EN/Publikationen/Digitale-Welt/handbook-regulatory-sandboxes.pdf?__blob=publicationFile&v=2), etc.

[88] See 2023 White Paper, as well as highlighted in C. NARDOCCI, *supra*.

of the law. Furthermore, it would build a bridge between the Member States (and their national specificities) and EU stakeholders, 'simplifying' and at the same time optimizing the EU's multi-level governance (by offering a *glocal* application of the law, also consistent with the EU's principle of subsidiarity). Overall, we need to rationalize the institutional landscape of digital-governance Authorities – reducing their number and, in any case, ensuring the highest possible degree of coordination – at both the national and EU levels, thereby simplifying and optimizing the EU's multi-level governance.

On the other hand, it must be realized that the "Competitiveness compass" requires creating a territory favorable to investment. Today, by contrast, the Union's stakeholders and, in general, those who have economic interests in the Union's digital market must deal with a multiplicity of different Authorities (each with its own rules and guidelines) for every different manifestation in the technological field (consider the competent authorities in matters of data, AI, cybersecurity, competition and the market, etc.). Each of these centers then provides different interpretations of the rules, depending on the sector of reference. Yet, as is well known, one of the pillars of the Union is the principle of legal certainty,[89] which finds in the preliminary reference its instrument of affirmation at the case-law level. In the digital field, however, this does not seem sufficient: the speed of technological evolution prevents effective recourse to centralized interpretation by the courts; and instead imposes uniform interpretation as quickly as possible (so as then to reach uniform application).

The EU is well aware of these needs,[90] but struggles to put them into practice. Regulatory simplification has been among the Union's priorities for some time, but routes such as the REFIT programme or the Digital Clearinghouse (in its original version and in the hypothesized 2.0) do not appear decisive.

In this respect, thinking of such initiatives as panaceas for the problems of digital regulation, it must be said that today the problem lies not so much in the technique of law-making (which would require a re-thinking/streamlining of the Union's legislative process) or of conflict resolution, but in the (lack of) prevention of those regulatory conflicts. Prevention must be attained through uniform interpretation of the rule, shifting towards a different reference point for normative interpretation. It is true that the EDPB intends to alleviate the burden of conflicts of interpretation and jurisdiction. Still, it cannot be considered acceptable to offload onto the EDPB a task that – by contrast – should belong to the EU Commission. The latter is, as is well known, the "guardian of the Treaties", which under Art. 17(1) TEU "shall ensure the application of the Treaties, and of measures adopted by the institutions", and "shall oversee the application of Union law" (albeit under the control of the Court of Justice); as it is also the body that can act under Art. 258 TFEU to ensure the uniform application of EU law, and can (Art. 291 TFEU) adopt "implementing acts" to specify how to apply a rule. All the more so since, on closer inspection, identifying the Commission as the sole interpreter – at the centralized level – of the rules, would allow the EU itself to streamline and render more effective the enforcement process of its digital regulation (and thus respond to one of the major problems that – as we have seen – afflict the European ecosystem). For the same reasons, reforms should include direct challengeability of EDPB decisions before the CJEU and the adoption of majority voting to streamline decision-making and enhance legal certainty.

[89] M. L. TUFANO, *La certezza del diritto nella giurisprudenza della Corte di giustizia dell'Unione europea*, in *Il Diritto dell'Unione Europea*, 2020.

[90] As already emerges by the EU Commission, *Better Regulations Guidelines*, Nov. 2021.

The aforementioned implementing acts and delegated acts[91] can then serve to achieve the flexibility that had already been identified as necessary by the Better Regulation Guidelines ("flexibility within the reporting period"; "'trading' across policy areas"; "exemptions in certain exceptional circumstances"): delegated acts should become the natural venue for updating the annexes to regulation (containing thresholds, technical lists, formats, and classification criteria), so as to be able to update them easily as technology changes, avoiding legislative reopenings and national divergences on the "when/how" of updating. Through implementing acts and comitology, national administrative adjustments could be harmonized; as well as where multiple policies require coordinated implementation (e.g., digital: DSA/DMA/AI Act), implementing acts (forms, glossaries, calendars) could be used more quickly to avoid overlaps and double compliance.

Delegated acts allow rapid and legislature-controlled technical updates, while implementing acts allow operational uniformity through comitology; more transparency, common standards and shared criteria; reducing margins of national interpretation, lowering compliance costs and limiting application heterogeneity.

This reading is also supported by the Data Act. The Regulation, which intends to create a European regulatory framework based on data sharing and on a fair data economy in the Union, immediately presented itself as bearing a revolutionary approach to data access,[92] a first decisive step towards a European Data Space (focusing not by chance – Chapter III – also on data sharing based on "fair, reasonable and non-discriminatory (FRAND) terms").[93] And indeed, the Data Act confers on the Commission the power to adopt delegated acts and to require European standardization organizations to develop harmonized standards that satisfy essential requirements on the interoperability of data, of data-sharing mechanisms and services, and of European common data spaces; confirming the relevance of such instruments.

The prevention of regulatory conflicts must become a distinct policy goal. Ex ante impact assessments for new initiatives in the digital field should systematically include a "coherence test" with existing regimes, supported by public, reasoned matrices indicating overlaps, derogations and coordination clauses. A sunset or review mechanism for certain high-friction obligations could avoid crystallising provisions that technological practice has shown to be disproportionate or ineffective. In this perspective, the idea of a "Digital Clearinghouse 2.0" regains sense only if reconceived as a permanent lab of anticipatory coherence, not as yet another layer in the bureaucratic palimpsest.

Such interventions are consistent with the Digital Package recently launched by the Commission,[94] confirming the opportunity for targeted action.

---

[91] It should come as no surprise that the European Commission has been given the power to adopt delegated acts with the aim of specifying the measures and other key indicators that will provide guidance on compliance for suppliers and deployers. Recent examples of this integrative role of the EU Commission are the two guidelines on prohibited AI practices and on the definition of AI systems.

[92] C. PERARNAUD, *The EU Data Act: Towards a new European data revolution?*, CEPS Papers 35693, Centre for European Policy Studies, 2022.

[93] Similarly to what can be said about data altruism for objectives of general interest (Art. 2(16), DGA).

[94] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/7568284-Digital-package-digital-omnibus-_en.

5.3. The Need for Investments

We must also rethink how to invest in innovation.

Investments, in this framework, are not an external corrective to an otherwise self-sufficient regulatory model. They are an integral part of the constitutional engineering of the digital Union. A legal order that demands high standards of compliance, explainability and safety must structurally accompany such demands with stable financing lines for SMEs and public administrations, European critical infrastructures that reduce dependency on non-EU providers, and large-scale programmes for AI literacy and regulatory literacy.

From a constitutional standpoint, the mismatch between the ambition of the AI Act and the modest level of human and financial resources dedicated to its implementation risks transforming fundamental rights rhetoric into an empty promise. If the Union truly believes that trustworthy AI, robust cybersecurity and effective data protection are conditions for preserving democracy and sovereignty, it must accept that such conditions have a cost and that this cost cannot be entirely shifted onto individual operators.

For this reason, future digital packages and the implementation of the Digital Decade targets should be explicitly tied to measurable commitments in three directions: reducing the cost of compliance per unit of innovative output (through simplification and standardisation); increasing public and blended investments in enabling infrastructures and skills; and monitoring, with independent evaluation, the distributive effects of digital regulation on different categories of actors. Only in this way can European digital constitutionalism avoid the trap of being simultaneously over-ambitious in normative rhetoric and under-effective in material outcomes.

First of all, with Communication n. 414/2022 the European Commission set the new simplification-oriented guidelines on granting State aid in favor of research, development and innovation, while the General Block Exemption Regulation has also included AI among the technologies compatible with State aid, exempt from notification obligations: thus showing recourse to State aid that – however – appear to be incentives, all the more in light of the unchanged framework in Art. 107 TFEU.

We also have to recognize the importance of AI literacy, which has by now become a structural component of the EU's digital policy: the AI Act requires providers and deployers to ensure an adequate level of AI literacy among personnel (Art. 4), while Article 3(56) specifies its content and purposes[95] and Recital 20 clarifies the systemic rationale: widespread literacy enables democratic oversight, informed choices, and risk reduction across the AI life cycle. AI literacy is not an ethical add-on, but a legal obligation.

At the same time, however, EU indicators empirically reveal a persistent gap. As noted before, in 2023 only 56% of citizens aged 16–74 had basic digital skills, 24 points short of the 80% target for 2030; at the same time, however, the job market is faring no better: ICT specialists numbered 9.8 million in 2023 (4.8% of employment) and exceeded 10 million in 2024 (5.0%), still well below the 20-million objective. A gender gap endures (approx. 19% women), and in 2024 57.5% of firms seeking ICT profiles reported hiring difficulties.

It is then mandatory to close the gap, if it is true – as it certainly is – that the ethics of technological society

[95] The general provisions apply from February 2nd 2025, with national competent authorities to be designated by August 2nd 2025 and supervision/market surveillance commencing on August 2nd 2026.

requires interdisciplinarity[96] and that a concerted effort[97] will be necessary. In the latest years, the EU architecture has tried to combine competence frameworks and financing levers: DigComp 2.2 (for citizens) and DigCompEdu (for educators) guide curriculum design, alongside ethical guidelines on AI and data in education. Financially, the Digital Europe Programme allocates €1.3 billion (2025–2027) to AI, cybersecurity, and digital skills (with a cumulative skills envelope of €580 million, 2021–2027); the RRF requires ≥ 20% digital spending in national recovery plans; and networks such as the Digital Skills & Jobs Coalition and the Pact for Skills support public–private partnerships for upskilling and reskilling.

Operationally, scholarship and policy documents suggest integrating compliance and pedagogy (mapping Article 4 requirements onto DigComp/DigCompEdu), tying investments to Digital Decade indicators and DIGITAL/RRF calls (prioritising micro-credentials and short, high-impact modules for public administrations and SMEs), institutionalizing teacher training (DEAP, ethical guidelines), measuring and improving with Eurostat indicators, and addressing territorial and gender gaps to reduce the mismatch between skills supply and demand.

To rapidly bridge the digital-literacy gap in the workplace and in the public administration, an "EU-wide" program that can achieve its goals in the short term (2–3 years) with short certified modules seems necessary; reducing compliance costs for enterprises and administrations, aligning training, safe use and competitiveness.

7. Conclusions. Re-Aligning Europe's Digital Constitutionalism

The trajectory traced in the preceding pages allows for a conclusive thesis: Europe's digital regulatory season can no longer be understood as a neutral technico-normative phase of sectoral adjustment. It constitutes, in all respects, a moment of constitutional redefinition of the European project. The cumulative effect of the GDPR, DSA, DMA, Data Act, DGA, NIS2, EHDS, the AI Act and the broader cybersecurity and platform framework is that of an unprecedented densification of public power over the digital environment, exercised at multiple levels and by a plurality of actors. This evolution, however, has occurred in the absence of an explicit and coherent constitutional grammar capable of governing overlaps, coordinating authorities, and reconciling the protection of fundamental rights with innovation, competitiveness and technological sovereignty. If not corrected, this asymmetry between regulatory ambition and systemic rationality risks turning what has been celebrated as the "Brussels Effect" into its own unintended reversal: a model perceived as normatively hypertrophic, economically dissuasive and institutionally opaque.

The first conclusion is therefore conceptual. The analysis confirms that the digital is not simply one of many policy domains, but a privileged field in which what doctrine has called "digital constitutionalism"[98] measures itself against the structural incompleteness of the European constitutional order. Constitutionalism in the digital age is characterised by the need to subject both public and private powers operating

[96] M. COECKELBERGH, *AI Ethics*, Cambridge (Mass.), 2020.

[97] A. D'ALOIA, *Intelligenza artificiale, società algoritmica, dimensione giuridica. Lavori in corso*, in *Quaderni costituzionali*, 3, 2022, 651-683.

[98] E. CELESTE, *Digital constitutionalism: a new systematic theorisation*, in *International Review of Law, Computers & Technology*, 33(1), 2019, 76-99.

in the digital environment to transparent, accountable and rights-compliant constraints and procedures. In this sense, the European Union has undoubtedly played a pioneering role, building a sophisticated catalogue of guarantees, from data protection to platform accountability. Yet it is also clear how digital constitutionalism requires not only the multiplication of guarantees, but also their systemic integration: a clear hierarchy of principles, coordination mechanisms among regimes, and institutional architectures that prevent conflicts of competences from morphing into structural irresponsibility. It is precisely on this point that the current European framework, as reconstructed above, reveals its most evident fragilities.

The second conclusion concerns method. The Union's regulatory approach to the digital has privileged an additive logic: new problems, new regulations. Not only could doubts arise about the correctness of this approach[99], but – moreover – this "regulatory layering" has produced multi-regulatory and multi-level enforcement concerns that are by now empirically manifest, as recognised not only in critical scholarship, but also in institutional self-diagnoses such as the State of the Digital Decade 2025, the Draghi Report on competitiveness and the Letta Report on the Single Market. The problem is not the ambition to regulate, but the absence of an ex ante constitutional technique of coherence: no general clause for conflict resolution between overlapping regimes; no systematic use of primary/subsidiary logics or integrated procedures (for instance, unified assessments and notifications for data protection, AI and cybersecurity); a fragmented galaxy of authorities and boards whose interactions are left to soft coordination rather than to a clear allocation of final responsibility.

From a constitutional law perspective, this mode of proceeding is untenable for at least three reasons. First, it erodes legal certainty and foreseeability, thereby affecting the effectiveness of rights and freedoms that presuppose predictable constraints and intelligible obligations. Secondly, it alters the proportionality calculus under Article 52(1) of the Charter: measures that may appear proportionate if assessed in isolation risk becoming excessive when considered in their cumulative impact on the same actors and processes. Thirdly, it feeds a form of "polycentric irresponsibility": the multiplication of regulators and forums blurs lines of accountability, both political and jurisdictional, and complicates judicial review (and in this sense, the cybersecurity regulation appears to be a perfect example of a field in which emergencies, fragmentation and expansion of supervisory powers test traditional constitutional categories).[100]

The third conclusion is normative and points to a constitutional recalibration along three axes, which emerge as conditions of sustainability for the European digital model. First of all, we need a Charter-centred balancing as binding technique, not rhetorical ornament. The Charter of Fundamental Rights, read in its systematic unity, must become the explicit matrix for interpreting and implementing digital regulation. This means rejecting any monistic reading that turns data protection into a meta-right structurally prevailing over entrepreneurial freedom, innovation and freedom of expression; or, conversely, any technocratic narrative that marginalises privacy and non-discrimination in the name of competitiveness. A genuine Charter-centred approach obliges the legislator and regulators to make the balancing choices

[99] M. RUOTOLO, *Il potere, tra pubblico e privato. Tracce per un dialogo tra civilisti e costituzionalisti*, in *Costituzionalismo.it*, 3, 2024, highlights the possibility of considering, for example, a transposition into the "digital world," with the necessary adaptations, of tools already used in other sectors: a "reconfiguration" of traditional law tools for application to private digital powers (a salso stated in L. TORCHIA, *Poteri pubblici e poteri privati nel mondo digitale*, , 1, 2024).

[100] E. C. RAFFIOTTA, *Cybersecurity regulation in the european union and the issues of constitutional law*, in *Rivista AIC*, 4, 2022.

transparent, subject them to proportionality review, and preserve the "essence" of all rights involved. The Union can then preserve its regulatory influence only if it demonstrates internally what it demands externally: coherence, enforceability, and reasonable burdens. The Draghi report, as well as economic analyses on the competitiveness gap in AI and digital infrastructures, converges in indicating complexity, fragmentation and uncertainty among the first obstacles to investment and scale-up in Europe: a constitutional response requires streamlining overlapping regimes through coordination clauses and integrated procedures; rationalising the enforcement architecture, reducing redundancies among authorities and clarifying tie-breaking and leadership roles in cross-border and cross-regime cases; enhancing the justiciability of key interpretive acts (guidelines, decisions of European boards and offices) before the Court of Justice, thus anchoring the evolution of digital law to a robust system of judicial control. In this perspective, digital constitutionalism becomes the terrain on which the Union measures its capacity to transform regulatory density into a factor of reliability rather than of deterrence.

Finally, the sustainability of the European model depends on its ability to align high normative expectations with adequate material support. Without investments in digital infrastructures, in public and private compliance capacities, in supervisory authorities and in skills, the sophisticated apparatus of guarantees risks producing a dual effect: on the one hand, it consolidates the position of large actors able to absorb compliance costs; on the other, it excludes SMEs, public administrations and civil society actors from the capacity to fully exercise and protect rights in the digital environment. Recent data on EU investments under the Digital Europe Programme and related initiatives move in the right direction but still appear insufficient when measured against the cumulative obligations introduced by the new regulatory packages. Constitutional discourse must therefore incorporate the distributive dimension of digital regulation: a model that is formally rights-enhancing but materially exclusionary would contradict the promise of a Union that is "highly competitive" and "social" at the same time.

On this basis, the conclusions of this analysis are deliberately ambivalent. On the one hand, they recognise the European digital strategy as a laboratory of constitutional innovation: few legal orders have attempted, with comparable systematicity, to subject technological development to a dense framework of fundamental rights, oversight mechanisms and public accountability. On the other hand, they underline that the same strategy has reached a point of saturation at which further additions to the normative edifice no longer increase its legitimacy but rather expose its structural limits. The alternative is not simply between regulation and deregulation, nor between rights and the market. It is between a digital Europe built through successive layers of sectoral interventions, and a digital Europe capable of reflecting constitutionally on itself: reordering its norms, clarifying its institutions, making explicit its priorities and trade-offs. If taken seriously, the proposals outlined – Charter-centred balancing, systemic simplification, institutional responsibility, and material support for compliance and innovation – are not a technocratic adjustment, but the substance of a European "digital constitutionalism" worthy of the name. They would allow the Union to preserve its regulatory vocation without sacrificing competitiveness; to affirm digital sovereignty without slipping into regulatory isolationism; and to protect fundamental rights not only in judicial rhetoric, but in the everyday life of citizens, administrations and enterprises that inhabit the European digital space. The challenge, ultimately, is political and constitutional before being technical: to decide whether Europe's digital future will be shaped by a coherent constitutional choice or by the inertia of its own regulatory successes.