The new balance between data circulation and data protection in the Digital Single Market*

di MARCO OROFINO**

SUMMARY: 1. Introduction: data as a complex legal asset. – 2. The evolution of the European approach to data free flow. – 3. Beyond protection: the Data Governance Act, the Data Act, the EHDS, and the AI Act. – 4. Regulated data circulation as a constitutional requirement for the Digital Society. – 5. Conclusions.

1. Introduction: data as a complex legal asset

In recent years, data governance has assumed a central role in economic, political and legal debates. Within an increasingly interconnected digital society – further accelerated by the ongoing AI revolution – the availability and the circulation of data can no longer be regarded merely as a technical issue or an economic resource underpinning global or regional markets. Rather data has acquired constitutional significance, as it is intrinsically connected to the effective exercise of fundamental rights.

The central claim advanced here, whereas data regulation was historically conceived and structured around personal data protection as a defensive right – primarily aimed at preventing intrusions into private life – the contemporary challenge lies in developing a governance model that enhances data usage while safeguarding dignity, equality, and individual autonomy. The need for data protection is by no means obsolete, the risks of intrusion into personal choices – and even into the capacity for self-determination – are constantly and dangerously increasing.

Nevertheless, this not diminish the necessity of a paradigm shift in regulatory approach.

This transformation, already significantly advanced, entails completing transition from a proprietary paradigm to one of openness

* The reflections developed herein are the outcome of the Net4Future research project carried out within the RESTART programme. The paper has not been subject to peer review, in accordance with the journal's editorial policies and in compliance with the ANVUR criteria set out in Article 2, paragraph 2, letter (c).

** Full Professor of Constitutional and Public Law, University of Milan.

grounded in shared responsibility, where algorithmic transparency, infrastructure security, and informed individual participation are paramount.

From a methodological perspective, this study adopts a constitutional lens, examining the evolution of the European legal framework on data through both its regulatory and its rights-based dimension.

The analysis proceeds along two main axes: first, by reconstruction the gradual shift from a defensive model of data protection to a governance-based approach that actively promote data circulation: and second, by assessing why this shift is not merely desirable for reasons of competition or economic efficiency, but constitutionally necessary for effective protection of fundamental rights in the digital society.

The expected outcome of this inquiry is twofold.

On the one hand, it highlights the emergence of a new "constitutional grammar" of data within the European Union, where circulation is no longer conceived solely as an economic tool but as a structural condition for rights. On the other hand, it shows how the Union, through instruments such as the GDPR, the Data Governance Act, the Data Act, the European Health Data Space, and the Artificial Intelligence Act, has assumed a leading role that transcends market regulation and points toward a new phase of European constitutional integration.

2. The evolution of European approach to data free flow

For a long time, the flow of information was regulated at the national level. Each country adopted its own rules governing the management, access, and protection of information held by public or private entities. To simplify this framework, the circulation of information managed by public administrations was restricted and governed by strict legal condition under national administrative law, while the circulation of information held by private parties fell within the scope of private and contract law. In each national legal system, specific restrictions were linked to the implementation of constitutional guarantees concerning privacy.

This fragmented yet broadly shared situation characterized most European countries prior to the intervention of the European Union.

Directive 95/46/EC marked the beginning of a harmonised European framework for the regulation of information flows, with particular

reference to personal data held by public or private entities[1].

Since the European Union is founded on the principle of free movement, the free movement of data emerged as a complementary requirement, ensuring coherence with the broader logic of the internal market.

At the same time, the free flow of data within the Union required a common level of protection, since member States had already begun to intervene unilaterally, thereby introducing barriers and undermining the logic of integration.

The logic of the Directive – at least in the way it was interpreted – was essentially defensive and rested upon a property-based model, exemplified by the primacy of consent among the conditions of lawful processing, the general prohibition on the processing of sensitive data under specific derogation, the enumeration of a series of data subject rights in which the proprietary logic clearly transpired, and the establishment of supervisory authorities focused on oversight.

Notwithstanding certain ideological emphases the approach adopted at that time was more than justifiable. It sought to strike a balance between data protection as fundamental right and data circulation as an economic instrument.

Over time, EU legislation expanded its scope beyond personal data. Subsequent interventions addressed data held by public sector bodies.

A new regulatory season was inaugurated by Directive 2003/98/EC on the re-use of public sector information[2]. It introduced, albeit with significant limitations, the principle of open public data. The main objective was to ensure the availability of data held by public authorities in order to support European businesses. At that stage, the free flow of data was still primarily regarded as an economic tool but it also began to be conceived as a means of fostering transparency and extend the control over the exercise of public powers

The emergence of a new function of the free flow of data become more evident with subsequent acts. Directive 2013/37/EU[3] and Directive (EU)

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 *on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, OJ L 281, 23.11.1995.

[2] Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 *on the re-use of public sector information*, OJ L 345, 31.12.2003

[3] Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 amending Directive 2003/98/EC *on the re-use of public sector information*, OJ L 175, 27.6.2013.

2019/1024[4] consolidated a culture of reuse grounded in accessibility, interoperability, cost-free availability, and the prioritisation of high-value datasets. These instruments also significantly expanded the scope of open data by narrowing the range of exceptions to disclosure.

Within this context, it should be noted that the new regulatory course continued to exclude personal data. The turning point occurred with the General Data Protection Regulation[5] (GDPR), which marked a genuine paradigm shift as evidenced by its very legal basis: it is grounded not only in Article 114 TFEU but also in Article 16, thereby placing data protection and the promotion of the free flow of data on an equal footing.

As widely emphasised in legal scholarship, the GDPR modernised the personal data framework through instruments such as accountability and co-regulation, privacy by design and by default, and mechanisms for assessing the compatibility between data processing and fundamental rights. More generally, it marked a first shift in the approach. no longer a regulation based on ownership but a regulation based on control.

Attempting to balance protection and circulation, one might say that the GDPR tried to be both a stern schoolmaster and a cheerful enabler. This duality is inherent in a context of shared responsibility, which necessarily requires a combination of flexibility and strict control.

In this broader framework, Regulation (EU) 2018/1807 on the free flow of non-personal data[6] further complemented the GDPR by addressing a different but equally strategic dimension. By prohibiting unjustified data localisation requirements and strengthening portability – particularly for professional users – it contributed to the construction of a genuinely integrated data economy within the Union.

Taken together, the GDPR and the Free Flow of Non-Personal Data Regulation represent the first attempt to design a comprehensive European legal environment in which the circulation of data, whether personal or non-personal, is promoted under conditions that simultaneously safeguard

[4] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 *on open data and the re-use of public sector information* (Open Data Directive), OJ L 172, 26.6.2019.

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 *on the protection of natural persons with regard to the processing of personal data and on the free movement of such data* (General Data Protection Regulation, GDPR), OJ L 119, 4.5.2016.

[6] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 *on a framework for the free flow of non-personal data in the European Union*, OJ L 303, 28.11.2018.

fundamental rights and ensure market efficiency. This dual structure laid the foundations for the subsequent legislative season, in which the Union explicitly embraced data as a strategic asset to be governed not only through protection but also through active promotion and valorisation.

3. Beyond protection: the Data Governance Act, the Data Act, the EHDS, and the AI Act

In the most recent phase, a significant wave of new regulations has been approved – among them the Digital Services Act (DSA)[7], the Digital Markets Act (DMA)[8], the Data Governance Act (DGA)[9], the Data Act (DA)[10], the European Heath Data Spaces (EHDS)[11], and the Artificial Intelligence Act (AIA)[12]. All of these acts introduce specific provisions on data circulation, including aspects of personal data circulation, thereby producing effects on the framework established by the GDPR.

While neither the DSA nor the DMA is a regulation on data (personal or non-personal) as such, both pursue the objectives of enhancing transparency and rebalancing the market by curbing excessive concentrations of power arising from data hoarding and exploitation control over data usage, and on the other, curbs the concentration of power arising from data hoarding and exploitation.

By contrast, the other instruments - the Data Governance Act, the Data Act, the European Health Data Spaces and to some extent, also the Artificial Intelligence Act – constitute genuine data regulations, as they establish substantive rules governing the circulation, sharing and re-use of data.

---

[7] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 *on a Single Market for Digital Services* (Digital Services Act), OJ L 277, 27.10.2022.

[8] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 *on contestable and fair markets in the digital sector* (Digital Markets Act), OJ L 265, 12.10.2022.

[9] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 *on European data governance* (Data Governance Act), OJ L 152, 3.6.2022.

[10] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 *on harmonised rules on fair access to and use of data* (Data Act), OJ L 2023/2854, 22.12.2023.

[11] Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 *on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/284*, OJ L, 2025/327, 5.3.2025.

[12] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 *laying down harmonised rules on artificial intelligence* (Artificial Intelligence Act), OJ L 2024/1689, 12.7.2024

Just a few examples illustrate this new approach. The DGA introduces a trust-based model for data sharing, promoting voluntary mechanisms such as data altruism and ensuring the fair re-use of data held by public bodies, including sensitive and personal data, under strict safeguards. It also regulates data intermediaries to foster reliable infrastructures for data access and re-use, laying the foundation for common European data spaces like the European Health Data Space (EHDS). This regulation is highly significant, both for its own objectives and for the argument advanced in this study, as it directly impacts the rules governing the circulation of health data—classified under the GDPR as "sensitive" or "special category" data.

According to Article 9 GDPR, such data may only be processed under one of the exceptions to the prohibition set out in paragraph 2. The EHDS provides a specific legal basis for both the primary and secondary use of health data, thereby moving beyond reliance on individual consent.

The Data Act, with a more private-law orientation, empowers users of connected devices to access and share the data they generate, thereby reinforcing the principle of user control over personal data. These rights are both contractual and rooted in the public interest, as they complement the fundamental right to data protection under the GDPR.

The Act is particularly significant, both for its own objectives and for the argument advanced in this study, since it directly affects the rules governing the circulation of all data—including those falling under the GDPR's special categories of personal data, which are generally subject, pursuant to Article 9, to narrowly defined exceptions to the prohibition of processing.

At the same time, the DA embodies the principle of data circulation as a constitutional requirement, ensuring that information produced in the digital environment does not remain locked within proprietary silos but can circulate under fair and secure conditions, thereby sustaining innovation, market integration, and the effective enjoyment of fundamental rights.

Taken together, the DGA, the DA, and the EHDS—building on the governance model introduced by the DGA—mark a shift from a merely protective approach toward a governance-based framework. This evolution does not simply balance innovation, personal data rights, and societal interests at the regulatory level, but reflects a deeper constitutional reorientation: the circulation of data is recognised as a necessary condition

for the effective enjoyment of fundamental rights in the digital society.

They function as enabling pillars for regulated and secure data circulation, aligned with the GDPR but pushing beyond its protective framework to support Europe's broader goals of digital sovereignty and responsible data economy. Importantly this evolution, in line with the Union's official policy documents, emphasises that the use of data must serve the protection and effective enjoyment of fundamental rights.

The same approach can be found in the AI Act, which establishes a risk-based regulatory model for artificial intelligence. The Act explicitly links this model to both the free movement of AI-based goods and services and the protection of fundamental rights, as emphasised in its recitals[13].

Concrete examples of this favor for data circulation can be found in multiple provisions of the Act, ranging from rules on data governance and dataset quality to those on testing, post-market monitoring, and the functioning of regulatory sandboxes. Article 10 requires high-risk AI systems to rely on high-quality training, validation, and testing datasets under strict conditions, including – where strictly necessary – the processing of sensitive personal data, always subject to appropriate safeguards. Article 59 further permits the use of personal data in regulatory sandboxes for the development, testing, and validation of AI systems, provided this takes place under controlled and lawful conditions. In addition, Article 61 on post-market monitoring obliges providers of high-risk AI systems to collect and analyse operational data after deployment in order to ensure ongoing compliance, thereby reinforcing the principle that data must circulate within secure and accountable frameworks. Similar obligations of documentation and transparency, scattered across other provisions of the Act, equally presuppose and promote the regulated sharing and accessibility of data. Taken together, these provisions demonstrate that the Act adopts a clear pro-circulation stance: since artificial intelligence cannot operate effectively without broad access to and sharing of data, the Union's objective is not to restrict circulation but to promote it within a framework of legality, security, and fundamental rights protection.

[13] See Recital 5 AI Act: «This Regulation aims to improve the functioning of the internal market by laying down a uniform legal framework for the development, the placing on the market, the putting into service and the use of artificial intelligence in conformity with Union values, supporting the free movement of AI-based goods and services across borders…».

4. Regulated data circulation as a constitutional requirement for the Digital Society

The analysis conducted so far suggests that an ongoing shift is taking place from a dichotomic approach - protection versus circulation – to a governance-based model. What remains to be clarified, however, is why such a change is not only desirable in order to promote competition and foster European economy but constitutionally necessary.

The concept of regulated circulation—promoted by recent European regulations—is therefore pivotal: only a system that guarantees accessibility and reusability of data, while respecting principles of security, transparency, and fairness, can support the effective realisation of rights in the digital society

In fields such as healthcare, education, mobility, and digital services, the capacity to access and share data – under clear rules of interoperability, transparency, and security – constitutes the very condition for making rights effectively actionable. While this holds true across all sectors, in some domains its relevance becomes immediately visible.

The protection of fundamental rights has always been technologically bound. We would not, for instance, regard it as compatible with the right to education (art. 14 EU CFR or art. 34 It. Const.) for students to pursue their studies in caves rather than in heated schools or in contemporary terms, even in classrooms devoid of digital tools such an interactive whiteboard. Nor would we consider it compatible with the right to healthcare (Art. 35 EU CFR or art. 32 It. Cost) for a broken leg to be cast without an X-ray, relying solely on clinical judgment or for a cruciate ligament to be operated on without arthroscopy.

The same reasoning applies in other domains. The right to work and fair working conditions (Arts. 15–16 EU CFR; Art. 4 It. Const.) increasingly depends on digital platforms and labour-market data, including systems for matching workers with opportunities and monitoring workplace risks. The right to social security and assistance (Art. 34 EU CFR; Art. 38 It. Const.) presupposes interoperable databases to manage welfare benefits, prevent fraud, and ensure portability of rights across borders. The right to freedom of movement and residence (Art. 45 EU CFR; Art. 16 It. Const.) requires the secure exchange of personal, biometric, and administrative data across Member States to make mobility effective. Even the right to effective judicial protection (Art. 47 EU CFR; Art. 24 It. Const.) increasingly relies on digitalised judicial files,

interoperable case-law databases, and AI-assisted tools that demand structured access to data.

Technology thus reshapes what we understand to be the essential content of a right.

In the health sector, concrete illustrations of the importance of regulated circulation include electronic health records, epidemiological surveillance systems, interoperable databases enabling early diagnosis, personalised treatments, and continuity of care, as well as numerous AI-based applications already available across medical disciplines.

Artificial intelligence technologies, in particular, promise new opportunities and are likely to expand what we consider to be the essential content of fundamental rights. Yet these technologies depend on data – they cannot function effectively without it. This is why the circulation of data is not merely a regulatory matter but ultimately a constitutional one: without meaningful access to data, many fundamental rights risks remaining purely formal rather than substantively guaranteed.

If the circulation of data becomes a precondition for the guarantee of fundamental rights, further constitutional issues inevitably arise. These principles can only be outlined here without the possibility of an extensive discussion, but their relevance to the constitutional nature of data circulation is undeniable.

It is closely linked, first, to the principle of substantive equality (Arts. 20–21 EU CFR; Art. 3(2) It. Const.), which requires the removal not only of legal but also of technological and infrastructural barriers that hinder effective participation in social, political, and economic life. It is also connected to the principle of solidarity (Art. 2 TEU; Arts. 31–34 EU CFR; Arts. 2 and 38 It. Const.), understood as a collective duty to ensure access to the digital tools and data flows that sustain welfare and citizenship. Finally, it resonates with the principle of economic, social, and territorial cohesion (Art. 174 TFEU; implicitly reflected in Arts. 2 and 3 It. Const.), which requires that digital fragmentation and asymmetries in access to data do not exacerbate geographical or socioeconomic divides.

Beyond equality, solidarity, and cohesion, other constitutional concerns may also be mentioned. Among them are the principles of dignity and personal autonomy (Arts. 1 and 8 EU CFR; Art. 2 It. Const.), the protection of freedom of expression and information (Art. 11 EU CFR; Art. 21 It. Const.), the conditions for democratic participation, the principles of proportionality and limitation of public powers (Art. 52 EU

CFR; Art. 97 It. Const.), and finally the right to effective judicial protection (Art. 47 EU CFR; Art. 24 It. Const.).

Each of these principles, although not explored here in detail, is deeply intertwined with the constitutional implications of data circulation.

5. Conclusions

The analysis conducted has sought to demonstrate that the European legal framework on data has undergone a profound transformation: from a defensive model centred on personal data protection, to a governance-based approach in which the circulation of data is actively promoted under regulated conditions. This evolution has been gradual, beginning with the harmonisation introduced by Directive 95/46/EC, consolidated through the GDPR and the Regulation on the free flow of non-personal data, and culminating in the most recent package of measures—the Data Governance Act, the Data Act, the European Health Data Space, and the Artificial Intelligence Act.

What emerges is a new constitutional grammar of data: circulation is no longer conceived merely as an economic tool, but as a precondition for the effective exercise of fundamental rights. Health, education, mobility, and democratic participation increasingly depend on secure, transparent, and fair access to and reuse of data. In this sense, regulated data circulation has become a constitutional necessity, closely tied to principles such as equality, solidarity, and cohesion, and deeply interwoven with dignity, autonomy, freedom of expression, proportionality, and judicial protection.

The European Union's legal order is thus moving beyond the traditional opposition between protection and circulation. It is embracing a model of shared responsibility, in which rights are safeguarded not only by shielding individuals from risks, but also by enabling their substantive enjoyment through structured access to data. This shift entails both opportunities and challenges: ensuring that technological development serves fundamental rights, preventing new inequalities, and avoiding excessive concentrations of informational power.

Ultimately, the constitutional imperative of our digital society is clear: without meaningful, regulated, and secure data circulation, fundamental rights risk remaining purely formal. With it, they can be realised in their full substantive dimension.

In this perspective, the European Union emerges as a constitutional actor in its own right: its intervention in the field of data goes well beyond the regulation of markets, amounting instead to a new step in the process

of European integration. By framing data circulation not merely as an economic resource but as a condition for the effective enjoyment of rights, the Union reshapes the very grammar of constitutional law in the digital age, reinforcing its role as both a guarantor of fundamental rights and a driver of political and social cohesion.