fypl
french yearbook *of* public law
Issue 2, 2024

The Public Administration of Data in the Italian Legal Order: Legal Framework, Fragmentation and Prospects for Reform

Pier Marco Rosa Salva
Post-doc in Administrative law, University of Udine

Abstract:

This article examines the public administration of data in the Italian legal order, where the data has become a structural element of administrative action rather than a mere by-product of the digitalisation of documents. It first reconstructs the European Union framework, showing how four regulatory logics (protection, circulation and re-use, data-as-infrastructure and algorithmic control) have successively shaped the data held by public authorities without ever being fully coordinated. It then turns to the Italian transposition, which is dispersed across the Digital Administration Code, the National Digital Data Platform, the rules on the opening and re-use of data and the law on the protection of personal data, and which has never been consolidated into a unitary body of rules. Two sectoral fields, healthcare and land governance, illustrate the resulting fragmenta-

tion, before the structural weaknesses of the national system (organisational dispersion, lack of capacity and technological dependence) are assessed. The article concludes by arguing for the recognition of the administration of data as an autonomous public function and by outlining the corresponding prospects for reform.

Keywords:

Public administration of data, Data governance, Digital Administration Code (CAD); Interoperability, Open data and re-use, Personal data protection

I. Data as a resource of public action and the transformation of the regulatory framework

The progressive centrality of data in public action is one of the most conspicuous features of the transformation that has been reshaping the administration over the last two decades.[1]

Today administrations hold an unprecedented quantity of data, from which a range of information may be drawn (on residence, taxation, health, territory and the environment) whose production, retention, circulation and use is becoming an ever more significant component of public activity, whether it concerns the provision of services or the adoption of measures and regulatory acts. Data are relevant from planning through to policy evaluation, and from the delivery to the oversight of the functions and activities carried out; they may contribute to securing the sound conduct, impartiality and transparency of public action, but also its accountability.[2]

These are features that, in the Italian legal order, are by now fully established and are the object of strategies and documents designed to plan the development and innovation of the organisation and action of the administration: the Three-Year Plans for Information Technology in Public Administration (*Piani triennali per l'informatica nella pubblica ammin-*

1 On data in public action, see, among the many contributions, Carullo, G., *Dati, banche dati e interoperabilità dei sistemi informatici nel settore pubblico*, in Cavallo Perin, R., Galetta, D.-U. (eds.), *Il diritto dell'amministrazione pubblica digitale*, 2025, Turin, Giappichelli, p. 257 ff.; Auby, J.-B., *Données publiques*, in *AD*, 2018, p. 109; Carullo, G., *Gestione, fruizione e diffusione dei dati dell'amministrazione digitale e funzione amministrativa*, 2017, Turin, Giappichelli; Falcone, M., *«Big data» e pubbliche amministrazioni: nuove prospettive per la funzione conoscitiva pubblica*, in *Riv. trim. dir. pubbl.*, 2017, no. 3, p. 601; Carullo, G., *Big Data e pubblica amministrazione nell'era delle banche dati interconnesse*, in *Conc. e mer.*, 2016, no. 23, p. 181; Falcone, M., *Dati aperti e diritto al riutilizzo delle informazioni: la declinazione italiana del paradigma degli open data*, in Ponti, B. (ed.), *Nuova trasparenza amministrativa e libertà di accesso alle informazioni*, II, 2016, Rimini, Maggioli; Bonomo, A., *Informazione e pubbliche amministrazioni: dall'accesso ai documenti alla disponibilità delle informazioni*, 2012, Bari, Cacucci; Marongiu, D., *I dati delle pubbliche amministrazioni come patrimonio economico nella società dell'informazione*, in *Inf. dir.*, 2008, no. 1-2; Ponti, B. (ed.), *Il regime dei dati pubblici. Esperienze europee e ordinamento nazionale*, 2008, Rimini, Maggioli; Cardarelli, F., *Le banche dati pubbliche: una definizione*, in *Dir. inf.*, 2002, no. 2, p. 321.

2 At the definitional level, it is in fact appropriate to distinguish the data, understood as an elementary informational unit, recorded in digital form and amenable to automated processing, from information, which presupposes an operation of contextualisation and attribution of meaning. See in this regard also Carullo, G., *Dati, banche dati e interoperabilità dei sistemi informatici nel settore pubblico*, cited above, pp. 258-259.

istrazione), which have followed one another since the 2017-2019 edition, have progressively shifted their focus from the digitalisation of the document to the regulation of public information assets, until, in the 2024-2026 edition, they addressed the integration of data and artificial intelligence in a systematic manner. From the paper archives of the past, the system is now moving towards an entirely different dimension, in which vast sets of information become immediately available and usable, including simultaneously and for different purposes.[3]

In the same regulatory field, a series of successive amendments, notably concerning the interoperability of databases and the circulation and re-use of public-sector information, has progressively reoriented the regulation of public information assets, largely in implementation of the European framework, posing a challenge to the public administration itself in terms of the reorganisation and development of the resources and skills needed to confront and manage this new digital dimension, in which a plurality of data of different nature and provenance must be correctly managed, used and preserved.

Moreover, the types of data relevant to public action are themselves diverse, according to the well-known distinctions drawn by legislation and scholarship: personal data and non-personal data, first of all, in accordance with the fundamental distinction now delineated at European level by Regulation (EU) 2016/679; public data, understood as data produced or held by a public administration in the exercise of its functions, and private data of public relevance, a category that has emerged more sharply in more recent European legislation; raw data and processed data; structured data and unstructured data.[4]

Alongside these classifications, others have developed, such as those of *big data* and *open data*, which are however of a different nature. The former designates a predominantly technological phenomenon, relating to the quantitative dimension of the data at stake and lacking any statutory definition; the latter, by contrast, constitutes a legal category, introduced into the Italian legal order by the Codice *dell'amministrazione digitale* (Digital Administration Code) enacted by d.lgs. 82/2005 and built around the opening and re-use of public data. It is the latter that is in part absorbed and redefined by the European logic of common data spaces, which replaces the open/closed dichotomy with a more elaborate scheme.[5]

3 The Three-Year Plans for Information Technology in Public Administration are provided for by Art 14-bis, para 2, point (b), of d.lgs. 82/2005, which entrusts their drafting to the *Agenzia per l'Italia digitale* (Agency for Digital Italy, AgID), reserving their approval to the President of the Council of Ministers or to the delegated Minister. The successive editions were approved, respectively, by d.P.C.M. of 31 May 2017 (Plan 2017-2019), d.P.C.M. of 17 July 2020 (Plan 2020-2022) and d.P.C.M. of 3 Dec. 2024 (Plan 2024-2026), to which the annual updates are then added. The edition in force and the updates are available at https://www.agid.gov.it/it/agenzia/piano-triennale.

4 On the classifications of the types of data relevant in the public sector, see Carullo, G., *Dati, banche dati e interoperabilità dei sistemi informatici nel settore pubblico*, cited above, p. 258 ff., who relates them both to the distinctions introduced by the Green Paper on public-sector information and to the sectoral definitions laid down by European and national legislation; see also Cardarelli, F., *Le banche dati pubbliche: una definizione*, cited above.

5 For the notion of *open data*, received by Art 1, para 1, point (l-ter), of d.lgs. 82/2005, and for its conceptual autonomy from the technological phenomenon of *big data*, see Carullo, G., *Dati, banche dati e interoperabilità dei sistemi informatici nel settore pubblico*, cited above, p. 261 ff., and Galetta, D.-U., *Open Government, Open Data e azione amministrativa*, in *Istituzioni del Federalismo*, 2019, no. 3, p. 663 ff.; on *big data* in the public sector see also the references at the beginning of Section I.

This matters because each of these categories (and in particular those to which specific burdens, obligations and processing arrangements are attached) entails direct repercussions on the action and organisation of the public administration, which is called upon to structure itself so as to manage them in a coherent and lawful manner. Beyond the mere transposition onto the digital sphere of administrative acts, in keeping with the original conception of the digital transition, the system is in fact progressively converging on a data-driven model, in which the data is no longer merely the content of a document but becomes itself a constituent element of the public information infrastructure and a functional basis.

It is onto this framework that, most recently, artificial-intelligence technologies are grafted: the training, validation and deployment of algorithmic systems depend decisively on the availability, quality and organisation of the public information assets, so that the regulation of data is reflected in the lawfulness and effectiveness of the decision-making processes in which such systems are employed.[6]

In the face of this centrality acquired by the data and of the speed with which European law is redefining its regulation, the Italian legal order presents a body of rules that has grown over time (through amendments to d.lgs. 82/2005, sectoral interventions, programmatic acts and soft law) in the absence of a clear, complete and up-to-date unitary framework capable of coordinating and holding together the different strands of the rules: the protection of personal data, transparency, re-use, interoperability and artificial intelligence.

This contribution therefore sets out to show how this regulatory stratification produces a fragmentation of the rules, liable to affect the effectiveness of the governance system for public data and, consequently, the capacity of the administration to manage its own public information assets—beginning, first of all, with the European Union framework.

II. European Union law: from the logics of protection to those of infrastructure

European Union law represents one of the principal sources of transformation of data

6 On the recourse to artificial intelligence in public action, see, among the many contributions, Gardini, G., Ricci, A., Ferrara, M.D., De Donno, M. (eds.), *Nuove tecnologie per nuove amministrazioni*, 2025, Turin, Giappichelli; Galetta, D.-U., *Artificial Intelligence and Public Administration. A Journey*, 2025, Naples, Editoriale Scientifica; Cavallo Perin, R., Galetta, D.-U. (eds.), *Il diritto dell'amministrazione pubblica digitale*, cited above; Galetta, D.-U., Hoffmann, H.H.C., Ziller, J., *Automazione, IA e pubblica amministrazione, fra diritto interno e diritto UE*, in Cavallo Perin, R., Galetta, D.-U. (eds.), *Il diritto dell'amministrazione pubblica digitale*, cited above; Torchia, L., *Lo Stato digitale. Una introduzione*, 2025, Bologna, Il Mulino, p. 117 ff.; Carloni, E., *Critica dell'amministrazione artificiale*, 2025, Bologna, Il Mulino; Sgueo, G. (ed.), *Governare (con) le macchine. Intelligenze artificiali generative e pubbliche amministrazioni*, 2025, Soveria Mannelli, Rubbettino; Lalli, A. (ed.), *La regolazione pubblica delle tecnologie digitali e dell'intelligenza artificiale*, 2024, Turin, Giappichelli; Cerrillo Martínez, A., Di Lascio, F., Martín Delgado, I., Velasco Rico, C.I. (eds.), *Inteligencia Artificial y Administraciones Públicas: una triple visión en clave comparada*, 2024, Madrid, Iustel; Di Martino, A., *Tecnica e potere nell'amministrazione per algoritmi*, 2023, Naples, Editoriale Scientifica; Previti, L., *La decisione amministrativa robotica*, 2022, Naples, Editoriale Scientifica; Cavallo Perin, R. (ed.), *L'amministrazione pubblica con i big data*, 2021, Turin, Università di Torino; Corradino, M., *Intelligenza artificiale e pubblica amministrazione: sfide concrete e prospettive future*, in www.giustizia-amministrativa.it, 2021.

regulation in the legal orders of the Member States, including as regards the action of public administrations.[7]

Data has progressively come to prominence in different respects, starting with the rules that concentrated on personal data, on their protection and on the safeguarding of the rights of the data subject, culminating in the General Data Protection Regulation No 679/2016 (GDPR). In a second phase the perspective broadened: the data was taken up as an economic and infrastructural resource, the object of rules governing its circulation, re-use and interoperability, both within the public sector and in public-private relations. Most recently, attention has shifted to the systems that operate on data, in particular artificial-intelligence systems, the requirements for whose development, placing on the market and use European law now regulates, including where they are applied in the action of public authorities.

A turning point in this broader perspective may be traced to the *European Strategy for Data* of 2020, by which the Commission set out the programme for the realisation of a single market for data, expressly linking their availability and circulation to the strengthening of the Union's competitiveness, to digital sovereignty and to the effectiveness of individual rights.[8]

The public sector is identified as a decisive juncture, both for the value of the information assets that administrations hold and for the driving role that their action can exercise over the circulation and re-use of data. That strategy produced a series of acts (such as the Data Governance Act, the Data Act, the sectoral regulations on European data spaces and the regulation on artificial intelligence) which, together with the GDPR and the established rules on public-sector information, have within a few years reconfigured the framework in which administrations produce, retain, exchange and re-use data.[9]

7 On the influence of European rules upon national legal orders, in particular starting from the field of data protection, see Bradford, A., *The Brussels Effect: How the European Union Rules the World*, 2020, Oxford, Oxford University Press. More broadly on the European rules on the digital sphere, see Pizzetti, F. (ed.), *La regolazione europea della società digitale*, 2024, Turin, Giappichelli.

8 See the Communication from the Commission, *A European Strategy for Data*, COM(2020) 66 final, of 19 Feb. 2020, which forms part of the digital package presented by the Commission on the same date, comprising the framework communication *Shaping Europe's Digital Future* (COM(2020) 67 final) and the *White Paper on Artificial Intelligence. A European Approach to Excellence and Trust* (COM(2020) 65 final). From its introduction, the Strategy identifies data as 'a central element' of the digital transformation under way and takes as its objective the construction of a genuine single market for data, organising its action around four pillars: a cross-sectoral governance framework for access to and use of data, the strengthening of infrastructures and processing tools, the development of skills and the identification of common European data spaces in strategic sectors.

9 The significance of the public sector emerges in several passages of Communication COM(2020) 66 final. In a first respect, administrations are taken to be holders of information assets of particular value, the object of specific consideration with reference to high-value datasets and to the coordination with the rules on the opening of public-sector data. In a second respect, public administrations are recognised as having a decisive role in the construction of common European data spaces: the Strategy identifies a plurality of strategic sectors in which such spaces are to be developed (among them health, mobility, energy, the environment, agriculture, finance, skills and manufacturing) and specifically envisages a 'common European data space for public administration', identified as an instrument for strengthening the transparency, accountability and quality of public spending, for combating corruption, for supporting the application of Union law and for the development of *govtech*, *regtech* and *legaltech* applications at the service of operators and of other services of public interest.

The relevance of public-administration data, and the logic of the circulation and re-use of data in EU law, were moreover acknowledged by the Commission as early as 1999 in the Green Paper *Public Sector Information: A Key Resource for Europe*, which identified in the information assets held by national administrations a strategic economic resource for European competitiveness and called for its value to be realised through harmonised forms of access and re-use.[10]

That document gave rise to a political and regulatory orientation that progressively developed and strengthened, first of all through Directive 2003/98/EC on the re-use of public-sector information, which marked its first binding enactment, laying down a minimum core of common rules (on non-discrimination, charging, exclusive arrangements, transparency and licensing) designed to remove the obstacles to the commercial and non-commercial re-use of documents held by the public bodies of the Member States. Directive 2013/37/EU then broadened its scope, introducing a general principle of re-usability of accessible documents.

The recast effected by Directive (EU) 2019/1024, on open data and the re-use of public-sector information, finally updated the framework to the changed technological context, highlighting in particular the category of dynamic data, the identification of high-value datasets subject to facilitated re-use, and the extension of the personal scope to public undertakings operating in regulated sectors.

This evolution, however, expresses only one of the regulatory logics with which Union law has addressed the data relating to administrative action: that of their circulation and exploitation as a resource.

It developed, however, in parallel with an older logic of a different character, namely the protection of personal data, which found in the GDPR its systematic culmination, following the earlier Directive 95/46/EC, which had been the first to establish at European level a harmonised framework for the protection of the natural person with regard to the processing of data concerning him or her, tying it both to the functioning of the internal market and to respect for fundamental rights and freedoms.

A. The logic of protection: Regulation (EU) 2016/679

The protection of personal data represents the first logic through which EU law developed; with the GDPR it sought to guarantee a uniform level of protection of the natural person with regard to the processing of data concerning him and, at the same time, to ensure the free movement of such data within the single market—both objectives enunciated in Article 1 and, indeed, already at the centre of the previous regime.

The Regulation—which on the one hand consolidates principles already traced, such as lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality and accountability (Article 5) in the processing of data, and on the other reinforces and develops the governance system for the processing of data, as illustrated by the data-protection impact assessment (Article 35), the

10 European Commission, *Public Sector Information: A Key Resource for Europe. Green Paper on Public Sector Information in the Information Society*, COM(1998) 585 final, 20 Jan. 1999, the document that opened a systematic reflection on the economic and democratic value of the information held by public administrations and on the conditions of its access and re-use, laying the conceptual premises of the path that would lead to Directive 2003/98/EC (the so-called PSI Directive, Public Sector Information).

principle of data protection by design and by default (Article 25), the role of the data protection officer (Articles 37-39), the regime for breaches and the notification obligation (Articles 33-34) and the turnover-based penalty framework (Article 83), always in a protective logic—also concerns the public administration.

The public administration is indeed identified, already by the provisions of the Regulation, as a controller of data-processing activities within the meaning of Article 4(7), operating, as a rule, on the legal bases of compliance with a legal obligation (Article 6(1)(c)) and of the performance of a task carried out in the public interest or in the exercise of official authority (Article 6(1)(e)). Those legal bases, pursuant to Article 6(2) and (3), nonetheless require a supplementary measure of Member State law identifying the controller, specifying the purposes, determining the types of data processed and the conditions of the processing.

The Regulation thus contributes to founding the legal bases for the processing of personal data according to a model of co-regulation between Union law and national law, which imposed within the domestic legal order a significant adaptation of the *Codice in materia di protezione dei dati personali* (Personal Data Protection Code) enacted by d.lgs. 196/2003, effected by d.lgs. 101/2018.[11]

This is, however, a regulatory logic that takes the personal data first and foremost as a projection of the person, and only secondarily as an object of possible circulation and economic use. Hence the identification of consent and of the other lawful bases as conditions legitimising a processing that, in their absence, would in principle be precluded, as well as of the rights of the data subject (Articles 15-22) as instruments of continuous control over the life-cycle of the data—all of this with the accountability of the controller, required no longer merely to comply with specific prescriptions, but to demonstrate on a continuing basis the adequacy of the technical and organisational measures adopted (Article 5(2) and Article 24 GDPR).

The protection of the personal data thus becomes a fundamental requirement, to be reconciled with the further logics of the exploitation of the data and information at the disposal of the public administration, giving rise to a tension in respect of which the European legislature has nonetheless provided—in regulating, through Directive (EU) 2019/1024, the opening of data and the circulation of the public information assets—a safeguard clause in Article 1(4), which preserves the regime of the GDPR and of the national provisions on the matter.[12]

11 This is, as is well known, pursuant to Art 4(1) GDPR, 'any information relating to an identified or identifiable natural person ("data subject")'. The data of legal persons therefore do not fall within it, whereas, as regards the data of natural persons connected to legal persons—such as, for example, the professional contact details of the legal representative—these continue to qualify as personal data where they allow the natural person to whom they refer to be identified, even indirectly, as clarified by recital 14 and confirmed by the case law of the Court of Justice (see, among others, CJEU, 9 Nov. 2010, Joined Cases C-92/09 and C-93/09, *Volker und Markus Schecke and Eifert*, and CJEU, 9 March 2017, Case C-398/15, *Manni*). The personal character of the data thus derives from its capacity to make a natural person at least indirectly identifiable, as provided by the same aforementioned provision, where it specifies that 'an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.

12 Directive (EU) 2019/1024 of 20 June 2019 on open data and the re-use of public sector information (recast). Art 1(4) provides that the Directive 'is without prejudice to Union and national law on the protection of personal data,

B. The logic of circulation and re-use

A second logic through which the EU rules have developed is that which identifies in the data held by the public sector a resource to be harnessed, including in economic, democratic and knowledge-development terms.[13]

In this regard, however, a distinction must be drawn between the dimension of external circulation from the administration, where the data flows into the market and into society, and the dimension of internal circulation, which also touches upon the question of interoperability, examined below (see II.C).

Focusing for the moment on the first aspect, which at the programmatic level likewise traces its roots to the aforementioned 1999 Green Paper, it found its first binding enactment in Directive 2003/98/EC, which laid down a minimum core of common rules designed to remove the obstacles to the commercial and non-commercial re-use of the information held by the public bodies of the Member States, affirming the right to knowledge as a 'basic principle of democracy' (recital 16).[14]

The rules then developed. As regards its material scope, it was progressively extended: from the generic notion of a document held by public bodies, to the inclusion of the holdings of libraries, museums and archives effected by Directive 2013/37/EU,[15] up to the prioritisation, in Directive (EU) 2019/1024,[16] which recast and replaced it, of dy-

in particular Regulation (EU) 2016/679 and Directive 2002/58/EC and the corresponding provisions of national law', and that 'the provisions of this Directive shall not affect in any way the level of protection of individuals with regard to the processing of personal data under the provisions of Union and national law, and in particular do not alter the obligations and rights set out in Regulation (EU) 2016/679'. The Directive was transposed into the Italian legal order by d.lgs. 200/2021, which amended d.lgs. 36/2006, the original implementation of Directive 2003/98/EC, on which see below in the text.

13 See on the subject Ponti, B. (ed.), *Il regime dei dati pubblici. Esperienze europee e ordinamento nazionale*, cited above; Gaspari, F., *L'agenda digitale europea e il riutilizzo dell'informazione del settore pubblico. Il riutilizzo dei dati ipotecari e catastali*, 2016, Turin, Giappichelli; see also, on the use of open data for transparency, Carloni, E., *L'amministrazione aperta. Regole strumenti limiti dell'open government*, 2014, Rimini, Maggioli. On the harnessing of open data for democratic participation, see Carullo, G., *Open Data e partecipazione democratica*, in *Istituzioni del Federalismo*, 2019, no. 3, p. 685 ff.

14 Directive 2003/98/EC on the re-use of public sector information, designed to 'harmonise the basic conditions' of re-use and to remove the principal obstacles that stood in its way in the internal market. It was transposed into the Italian legal order by d.lgs. 36/2006. Significantly, Art 2(4) of the Directive qualified the 'document' as 'any representation of acts, facts or information—and any compilation of such acts, facts or information—whatever its medium', with a deliberately broad notion, encompassing both documents in the traditional sense and structured data.

15 Directive 2013/37/EU on the re-use of public sector information, amending Directive 2003/98/EC, transposed by d.lgs. 102/2015, which amended d.lgs. 36/2006.

16 Directive (EU) 2019/1024 on open data and the re-use of public sector information (recast) overhauled and updated the previous rules, adapting them to the technological and organisational transformations of the decade following the adoption of Directive 2003/98/EC. Among the principal innovations are: the introduction of the category of dynamic data, to be made available for re-use immediately after collection through application programming interfaces (APIs) (Art 5); the identification of high-value datasets, entrusted to an implementing regulation and assigned to six thematic categories (geospatial data, earth observation and environmental data, meteorological data, statistical data, data on companies and company ownership, and mobility data), subsequently identified, in concrete terms, by Implementing Regulation (EU) 2023/138; and the extension of the personal scope to public undertakings operating in certain regulated

namic data and of high-value datasets, identified at the executive level as categories to which particularly favourable regimes of openness are to be assured. As regards its personal scope, beyond public administrations *stricto sensu*, public undertakings operating in regulated sectors were included. As regards the underlying principle, finally, the rules moved from the mere admissibility of re-use to a general principle of openness, so much so that it is no longer openness that must be justified, but its limitation.

This last directive does not, however, confine itself to permitting re-use, but imposes on the public administration active obligations as to format, cataloguing, accessibility, licensing conditions and charging regimes, transforming it from a holder of data into a supplier of a resource whose economic value it does not, save for exceptions, itself monetise. The relationship between the administration and its information assets is reversed: the data is no longer retained for the purposes of its administrative use, but is regarded as a potential *input* of an external economy.

This logic encounters, however, two limits. An internal limit, set by the logic of protection which—by virtue of the safeguard clause in Article 1(4) of Directive (EU) 2019/1024—ought to prevail over the logic of circulation, yet without any operational criteria being provided for reconciling the two, thereby shifting onto the controlling administration the responsibility for case-by-case balancing. And a structural limit, set by the fact that the rules on circulation regulate the *output* of the public administration, but presuppose, without however regulating it, the internal organisational transformation (quality, interoperability, data governance) needed for that output actually to be possible.

It is to this second limit that, at the European level, the rules centred on the more recent logic of treating data as infrastructure respond.

C. The logic of treating data as infrastructure

Starting from the *European Strategy for Data* of 2020, EU law developed according to a third and further regulatory logic, which no longer treats data as an object of protection or as a resource to be set in circulation, but focuses on the conditions under which circulation can actually take place. And this on the basis of the recognition that the opening of the public information assets, as constructed by the PSI trajectory, is not sufficient to generate value unless one has an ecosystem of interoperability, quality and shared governance of data.[17]

This logic has been articulated along three axes.

As regards intermediation and governance, Regulation (EU) 2022/868 (Data Governance Act, DGA)[18] introduced a harmonised framework for the re-use of data held by the

sectors and to data from publicly funded research (Art 1(1)(b) and (c)). The Directive was transposed into the Italian legal order by d.lgs. 200/2021, which amended d.lgs. 36/2006.

17 See, in Italian scholarship, Torchia, L., *Lo Stato digitale. Una introduzione*, cited above, p. 78 ff.; Resta, G., *Pubblico e privato nel sistema europeo di governo dei dati*, in *Rivista trimestrale di diritto pubblico*, 2022, no. 4, p. 971 ff.

18 Regulation (EU) 2022/868 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), applicable from 24 Sept. 2023, pursues the objective of strengthening the availability of data and trust in their sharing, addressing three principal aspects: the conditions for the re-use, by private parties, of certain categories of data held by public bodies and protected by third-party rights, commercial or statistical confidentiality or the rules on the protection of personal data (Chapter II); the regime of data-intermediation services, subject to a notification system and to neutrality obligations (Chapter III); and the rules on data-altruism organisations, understood as entities that

public sector that cannot be made available as open data (because protected by third-party rights, by statistical or commercial confidentiality or by the rules on the protection of personal data) regulating the conditions of their re-use for purposes of public interest, science or innovation.

As regards the availability of privately held data to the public sector, Regulation (EU) 2023/2854 (Data Act)[19] introduced rules on the sharing of data generated by connected products and related services, providing in particular for an obligation to make data available to the public sector in situations of exceptional need (Articles 14 et seq.), as well as obligations concerning technical interoperability.

As regards the construction of common spaces, European policies have set in motion the realisation of sectoral European data spaces, of which the *European Health Data Space*, the object of Regulation (EU) 2025/327, represents the first concrete implementation.[20]

The three axes combine into a circulatory governance that operates in both directions (from the public sector towards the market and from the market towards the public sector) and for specific sectoral fields.

As regards the public administration, this logic produces a transformation of role more radical than that induced by the PSI trajectory. Whereas the rules on re-use cast the public administration as a supplier of an informational output, the logic of treating data as infrastructure casts it as a node of a distributed architecture, in which it must interoperate with other public and private actors according to common technical and organisational rules, in order to make its data available even outside the open paradigm, and to exercise functions of intermediation and facilitation of sharing.

It is a transformation that affects not only what the public administration does with its data, but how it is itself organised, interoperability thereby becoming a structural requirement of the administration rather than an additional attribute of the data.

This logic, moreover, presupposes organisational and technical capacities that are not uniformly distributed either at the European level or within the national legal orders, with weaknesses that may prove pronounced, as is the case in the Italian legal order (see below, III).

collect data on a voluntary basis for purposes of general interest (Chapter IV).

19 Regulation (EU) 2023/2854 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), applicable from 12 Sept. 2025, regulates the sharing of data generated by the use of connected products and related services (Chapter II), introducing user access rights and mechanisms of portability to third parties. Of particular relevance, for the purposes of the relationship between data and public administrations, are the provisions of Chapter V (Arts 14 et seq.), which impose on private data holders obligations to make data available to public sector bodies, to the Commission, to the European Central Bank and to Union bodies in situations of exceptional need, in particular in the event of public emergencies or for the performance of specific tasks of public interest provided for by Union or national law. The Regulation also contains provisions on switching between data-processing services (Chapter VI) and on interoperability (Chapter VIII).

20 Regulation (EU) 2025/327 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847, which establishes the first binding sectoral European data space, structured around two axes: the primary use of electronic health data (care, continuity of treatment, patient access to their own data) and the secondary use (research, innovation, public-policy making, supervision), with the provision of national health-data access bodies for secondary-use purposes. The rules stand in a relationship of speciality vis-à-vis Regulation (EU) 2016/679, whose processing conditions they supplement for the health domain, and make the public health administration a node of a European architecture of interoperability between electronic health-record systems and between data catalogues for research.

D. The logic of algorithmic control

A fourth regulatory logic, of more recent formation, addresses data not as an object of protection, circulation or infrastructural use, but as the object of their algorithmic processing, in particular through artificial-intelligence systems.[21]

Regulation (EU) 2024/1689 (AI Act)[22] introduced in this respect a regulatory framework based on the classification of systems according to risk, and identified a core of specific obligations, of increasing intensity, for systems qualified as high-risk.

For the purposes of a public administration of data, the relevance of the AI Act may be appreciated along two dimensions. As regards scope, Annex III qualifies as high-risk a number of systems intended for use by or on behalf of public authorities, among them systems used to determine access to essential public benefits and services, to assess creditworthiness in certain conditions, to manage migration, asylum and border control, and to administer justice and democratic processes.

The public administration is therefore, in many of its most sensitive uses of AI, a direct addressee of the most stringent rules of the Regulation.

As regards the content of the obligations, the Regulation imposes, for high-risk systems, requirements that bear directly on the administrative organisation: the establishment of a risk-management system (Article 9), the governance of training, validation and testing data (Article 10), the technical documentation and the keeping of records (Articles 11-12), the provision of information to deployers (Article 13), human oversight (Article 14), and the requirements of accuracy, robustness and cybersecurity (Article 15).

Moreover, the GDPR already contained, in Article 22, specific rules on decisions based solely on automated processing that produce legal or significant effects on the data subject, recognising the latter's right not to be subject to them, save for the exceptions provided therein, and laying down minimum safeguards in terms of human intervention, the contestability of the decision and the right to express one's point of view. Such a provision has remained in force even after the AI Act, which operates on a different level, regulating the characteristics of the system and the obligations of the provider and the deployer. That said, the two sets of rules nonetheless partly concern the same aspects, in particular human oversight, without there being any provision expressly designed to resolve the problems of coordinating the application of the various texts.

E. The tensions between the regulatory logics

The rules adopted along these four logics stand in part on the same data and on the same

21 On the use of artificial intelligence in administrative action, see the contributions cited above, note 6.

22 Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence [...], of 13 June 2024, which adopts a risk-based approach distinguishing prohibited practices (Art 5), high-risk systems (Arts 6 et seq. and Annex III)—for which the requirements of Arts 9-15 are laid down—and systems subject to transparency obligations, providing for a staggered application over time of its provisions. See Pollicino, O., Donati, F., Finocchiaro, G., Paolucci, F., *La disciplina dell'intelligenza artificiale*, 2025, Milan, Giuffrè; Galetta, D.-U., *Artificial Intelligence and Public Administration. A Journey*, cited above, p. 193 ff.; Finocchiaro, G., *Diritto dell'intelligenza artificiale*, 2024, Bologna, Zanichelli; Malaschini, A., *Il Regolamento europeo sull'intelligenza artificiale (IA), l'orientamento italiano e i diversi indirizzi di Stati Uniti e Regno Unito*, in *Rassegna parlamentare*, 2024, p. 35; Marchetti, B., *Intelligenza artificiale, poteri pubblici e "rule of law"*, in *Rivista italiana di diritto pubblico comunitario*, 2024, p. 49.

aspects of administrative action, giving rise to possible overlaps and to tensions that EU law does not always reconcile.

The most evident is the structural tension between protection and circulation: the safeguard clause that makes the rules on personal data prevail resolves the hierarchy between the two logics, but offers no operational criteria of balancing, which remain entrusted to the controlling administration. To this are added the tension between data-as-infrastructure, which presupposes organisational and technical capacities that are not uniformly distributed, and that of algorithmic control, whose obligations overlap, without any express coordination, with those already flowing from the rules on protection.

Of these overlaps the European legislature now shows some awareness, given that the Digital Omnibus proposal, presented by the Commission in November 2025, envisages a consolidation of the open data directive, the Data Governance Act and the regulation on the free flow of non-personal data—texts that would be repealed and their rules merged into a restructured Data Act, as the single instrument for the data economy.[23]

This is an attempt to consolidate provisions that have stratified over time, in a perspective above all of competitiveness and simplification rather than of systematic coherence, and which for the time being concerns only the logics of circulation and of data-as-infrastructure.

Pending the development of this proposal, the European framework thus presents itself as a composite and not entirely coordinated arrangement, which national legal orders must not only transpose but hold together. And it is also under this aspect that the capacity of each legal order to translate the plurality of European logics into a coherent body of rules may be measured. In the Italian legal order, this translation has occurred progressively and sector by sector, without attempting any overarching harmonisation.

III. The national rules, between different sources and a plurality of purposes

If EU law has invested the data of administrative action according to distinct and not fully coordinated logics, the Italian legal order has not translated the body of rules adopted into a unitary design, but has received them by repeatedly amending texts already in force, each created for a purpose of its own and adapted over time to the development of the policies on the matter. The rules on public data have thus taken shape progressively and through different texts, without their being subsequently translated into a unitary body of rules.

The regime applicable to a given piece of data is therefore derived by coordinating provisions that have succeeded and overlapped one another over time and that respond to different purposes: from administrative efficiency, to economic valorisation, to transparency.

23 Proposal for a Regulation of the European Parliament and of the Council amending, among others, Regulations (EU) 2016/679 and (EU) 2023/2854 and Directives 2002/58/EC and (EU) 2022/2555, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150 and (EU) 2022/868 and Directive (EU) 2019/1024, the so-called 'Digital Omnibus', COM(2025) 837 final, of 19 Nov. 2025 (procedure 2025/0360(COD)). The package also comprises a proposal to simplify the rules on artificial intelligence (Digital Omnibus on AI), COM(2025) 836 final (procedure 2025/0359(COD)).

A. The Digital Administration Code and its evolution

In the Italian legal order, the general rules on data in administrative action are to be found first of all in the aforementioned *Codice dell'amministrazione digitale* (Digital Administration Code, CAD), enacted by d.lgs. 82/2005.[24]

The Code was conceived with the aim of gathering into a coherent body the rules on the use of information technologies in relations between administrations and between the latter and private parties. In its original structure, however, the data occupies a position ancillary to that of the electronic document: the rules are built around acts, around their formation, transmission and preservation, while information assets come to prominence above all as an effect of the digitalisation of documents.

The subsequent amendments (among which, d.lgs. 179/2016 and d.lgs. 217/2017) instead progressively enhanced the role of data, increasing its centrality within the system and developing the rules, for example, on the availability of the data of public administrations (Article 50), on open-type data and electronic access (Article 52), and on databases of national interest (Article 60).

These rules are in particular contained in Chapter V of the CAD, on 'Data of public administrations and digital identities, online applications and services', as articulated in Section I on 'Data of public administrations' and Section II on 'Usability of data'.

The principle is that of availability: the data of public administrations are formed, collected and preserved by means of technologies that allow their use and re-use, and each administration makes accessible and usable to others the data of which it is the holder, where their use is necessary for the performance of their institutional tasks, subject to compliance with the rules on the protection of personal data (Article 50); the transfer of data from one information system to another does not alter its ownership (Article 50, paragraph 3-bis).

Onto this structure three strands are embedded. *Openness*: the data and documents that administrations publish without the express adoption of a licence are deemed released as open-type data (Article 52). The qualification of certain collections as databases of *national interest* (Article 60): sets of information relevant to the performance of the functions of a plurality of administrations, among which, on first application, the national repertory of territorial data and the National Register of the Resident Population. And, finally, *interoperability*, entrusted to the National Digital Data Platform (Article 50-ter): a technological infrastructure designed to make possible the interoperability of the information systems and databases of administrations and of operators of public services, through interfaces gathered in a dedicated catalogue (addressed below, III.B).[25]

The components of the rules on the public information assets are therefore now

24 D.lgs. 82/2005, enacting the *Codice dell'amministrazione digitale* (Digital Administration Code). On the Code and its transformations, see, among others, Cardarelli, F., *L'uso della telematica*, in Sandulli, M.A. (ed.), *Codice dell'azione amministrativa*, 2017, Milan, Giuffrè, p. 421 ff.; Marchetti, B., *Amministrazione digitale*, in *Enc. dir., I tematici, Funzioni amministrative*, 2022, Milan, Giuffrè.

25 On the National Digital Data Platform, see Alberti, I., *La creazione di un sistema informativo unitario pubblico con la Piattaforma digitale nazionale dati*, in *Istituzioni del Federalismo*, 2022, no. 2, p. 473 ff.; Sandulli, A., *Lo «Stato digitale» pubblico e privato nelle infrastrutture digitali nazionali strategiche*, in *Rivista Trimestrale di Diritto Pubblico*, 2021, no. 2, p. 513 ff.; and, on informational interconnection in public contracting, Carullo, G., *Piattaforme digitali e interconnessione informativa nel nuovo Codice dei Contratti Pubblici*, in *federalismi.it*, 2023, no. 19.

found within the Code, even though they entered it progressively, without there having been any comprehensive revision of the rules. The result is a framework that addresses the various relevant aspects but does not appear to coalesce into a complete and systematic whole.

There is, moreover, a gap between the regulatory design and its implementation, as emerges for instance from the failure to adopt the National Data Strategy provided for in paragraph 4 of Article 50-ter CAD. That provision entrusted to a decree of the President of the Council of Ministers (to be adopted within 60 days, in agreement with the Ministries of Economy and of the Interior, after consulting the Data Protection Authority and obtaining the opinion of the Unified Conference) the task of establishing the strategy, identifying the types, limits, purposes and arrangements for making available the aggregated and anonymised data of which administrations are holders. Implementation, however, has followed an asymmetric path: the platform has become operational and the acts regulating its accreditation and functioning have been adopted, while the decree on the strategy does not yet appear to have been adopted.[26]

That the present framework is no longer adequate is, for that matter, acknowledged by the legislature itself, which by Article 11 of l. 167/2025 delegated to the Government the power to adopt, within 12 months, one or more legislative decrees for the simplification, amendment and integration of the Code, among other things precisely with a view to valorising and strengthening the public information assets, in addition to the processes of digitalisation of public administrations and the delivery of online services to citizens and businesses. Among the specific guiding criteria is that of 'guaranteeing and strengthening the interoperability of the information systems and databases of public administrations and of operators of public services', including through the simplification and rationalisation of the procedures for accessing data and for their availability through the services of the National Digital Data Platform (Article 11, paragraph 2, point (b)).[27]

A public consultation on the revision of the Code was also recently held, aimed at gathering proposals for simplification, amendment and integration with a view to the preparation of the new text.[28]

The decision to overhaul the structure of the Code thus appears to confirm how the progressive stratification of the provisions, including those relating to data, does not represent a coherent and overall evolution of the rules, but a limitation that still does not allow for the adequate regulation of one of the key sectors of the digital transition of the public administration.

26 In implementation of Art 50-ter there were adopted, among other acts, the d.P.C.M. of 22 Sept. 2022, laying down the obligations and time-limits for accreditation to the National Digital Data Platform, and the decree of the Under-Secretary of State to the Presidency of the Council of Ministers of 5 Dec. 2023, laying down measures for the implementation of Art 50-ter of d.lgs. 82/2005.

27 Law of 10 Nov. 2025, no. 167, on 'Measures for legislative simplification and the improvement of the quality of rule-making and delegations to the Government for simplification, reorganisation and reordering in certain matters', in *Gazzetta Ufficiale* no. 265 of 14 Nov. 2025.

28 The consultation 'Towards the new Digital Administration Code (CAD)', promoted by the Department for Institutional Reforms, by the Mission Structure for Legislative Simplification and by the Department for Digital Transformation, in agreement with the inter-ministerial Commission established by decree of 30 Jan. 2026, was held on the ParteciPa platform from 14 to 29 May 2026.

B. Interoperability and the National Digital Data Platform

To the European logic of data-as-infrastructure, the Italian legal order has responded principally with the *Piattaforma digitale nazionale dati* (National Digital Data Platform, PDND). Provided for in Article 50-ter CAD, introduced in 2017 and entirely rewritten in 2020, the platform is a technological infrastructure that seeks to make possible the interoperability of the information systems and databases of public administrations and of operators of public services: accredited entities share data and information through application programming interfaces, developed in conformity with the guidelines of the *Agenzia per l'Italia digitale* (Agency for Digital Italy, AgID) and gathered in a catalogue made available by the platform itself. Excluded are data relating to public order and security, to defence and national security, and to the judicial police and the economic and financial police (Article 50-ter, paragraph 3).[29]

The design is not that of a centralised database. The platform does not retain the information exchanged: each administration remains the holder of its own data and governs their use, while the infrastructure ensures the technical channel of the exchange, the identification of authorised entities and the traceability of accesses and transactions.

The most significant administrative effect is the strengthening of the once-only principle: data already held by one administration become effectively obtainable *ex officio* by others, giving effect to an obligation that the legal order has long known (Article 18 of l. 241/1990; Article 43 of d.P.R. 445/2000) but which had remained largely ineffective for want of technical support. Participation is not left to the choice of administrations: accreditation is compulsory and the relevant deadlines were fixed by the d.P.C.M. of 22 September 2022, while the platform has been operational since October 2022, within the framework of the NRRP investments in data and interoperability.[30]

As regards competences, the centralisation of these rules finds its foundation in the State's exclusive legislative power over the statistical and IT informational coordination of the data of the State, regional and local administrations (Article 117, second paragraph, point (r), of the Constitution): it is this title that allows uniform standards, languages and procedures to be imposed on a plurality of autonomous administrations, overcoming the management of information assets in non-communicating compartments.[31]

Yet it is precisely the nature of the instrument that marks a possible limit. The plat-

29 Art 50-ter was introduced by Art 45, para 2, of d.lgs. 217/2017, and was entirely rewritten by Art 34 of d.l. 76/2020, converted by l. 120/2020. On the evolution of the provision, see Sandulli, A., *Lo «Stato digitale» pubblico e privato nelle infrastrutture digitali nazionali strategiche*, cited above; Alberti, I., *La creazione di un sistema informativo unitario pubblico con la Piattaforma digitale nazionale dati*, cited above.

30 On the coordination between the platform and the exercise of the power of *ex officio* acquisition, see Alberti, I., op. cit., especially p. 484 ff. The guidelines on the technological infrastructure of the platform were adopted by AgID with determination no. 627/2021, on which the Data Protection Authority expressed its opinion of 16 Dec. 2021, no. 433.

31 On statistical and IT informational coordination as the foundation of State interventions in the matter, see again Alberti, I., op. cit., p. 487 ff.; Merloni, F., *Coordinamento e governo dei dati nel pluralismo amministrativo*, in Ponti, B. (ed.), *Il regime dei dati pubblici. Esperienze europee e ordinamento nazionale*, cited above, p. 153 ff. On the management of data according to 'siloed' logics, see Carloni, E., *Algoritmi su carta. Politiche di digitalizzazione e trasformazione digitale delle amministrazioni*, in *Diritto pubblico*, 2019, no. 2, p. 363 ff. On the gap between proclaimed interoperability and the standardisation actually practised, see Ponti, B., *Tre scenari di digitalizzazione amministrativa «complessa»: dalla interoperabilità predicata alla standardizzazione praticata*, in *Istituzioni del Federalismo*, 2023, no. 3, p. 599 ff.

form realises an infrastructure of exchange, which connects the systems but does not bear on the formation of the data. The ownership, quality, updating and legal qualification of the data remain with the individual administrations, so that interoperability rests upon information assets that remain fragmented upstream. And practical experience has shown the resistance of administrations to abandoning their own systems in order to migrate towards the common infrastructure, a resistance that neither the penalty mechanisms nor the reward mechanisms have entirely overcome.[32]

Technical connection is therefore not equivalent to legal integration: exchange presupposes common rules on the quality and the regime of the data exchanged, which the platform does not supply and which must be sought in the rules on openness and re-use (III.C) and on the protection of personal data (III.D).

C. The opening and re-use of public data

The European trajectory of circulation (II.B) was received into the Italian legal order through d.lgs. 36/2006, implementing Directive 2003/98/EC, progressively rewritten at each evolution of the European rules—first by d.lgs. 102/2015, for Directive 2013/37/EU, then, more incisively, by d.lgs. 200/2021, for Directive (EU) 2019/1024—until it became the general legislative reference on the opening of data and the re-use of public-sector information.

In the version in force, the decree proceeds from the principle whereby the documents held by public administrations and by bodies governed by public law (with the extension, deriving from EU law, to certain public undertakings and to data from publicly funded research) are re-usable for commercial and non-commercial purposes.

Availability is free of charge as a rule: charges, where provided for, may not exceed the marginal costs of reproduction, provision and dissemination, in addition to the costs of anonymising personal data and of protecting confidential commercial information (Article 7). Exclusive arrangements are permitted only in circumscribed cases, subject to periodic review and to publicity (Article 11). Dynamic data are made available through application programming interfaces immediately after collection, and high-value datasets, identified by Regulation (EU) 2023/138, are available free of charge, in machine-readable format and through the same interfaces. Implementation is provided for by the AgID guidelines (Article 12).[33]

The coordination with the Code is, however, not complete. The opening of public data is today regulated by at least three texts that overlap without any clear hierarchy: the CAD, which governs the formation of the data and establishes its release as open-type data in the absence of a licence (Article 52); d.lgs. 36/2006, which regulates re-use as a general regime; and d.lgs. 33/2013, which declares re-usable the data subject to mandatory publication (Article 7). Three perspectives (digitalisation, the market, transparency) thus converge upon the same data with non-coinciding definitions and purposes, and

32 On the resistance of administrations to adhering to the common platforms and on the prescriptive and incentivising mechanisms put in place to overcome it, see Sandulli, A., op. cit. The failure to comply with the obligations to make data available is relevant, among other things, for the purposes of the performance-related remuneration of the responsible senior managers.

33 The guidelines laying down technical rules for the opening of data and the re-use of public-sector information were adopted by AgID, pursuant to Art 12 of d.lgs. 36/2006, with determination no. 183/2023.

those applying the law are sent from one body of rules to another.[34]

The problem, therefore, arises not only from the coexistence of several sources, but from the fact that they qualify the same object, the public data, according to functions that do not always coincide: the data as an element of the digital organisation of the administration, the data as a resource open to economic and social re-use, and the data as an instrument of transparency and diffuse control. Fragmentation thus also takes on a functional character, since each set of rules presupposes a different way of acting on the part of the administration and a different relationship between the public information assets, the market and citizens.

Lastly, openness brings with it a competition-related aspect. Where public data feed downstream information markets, the holding administration finds itself in a position of de facto monopoly over the resource, and the conditions of access and charging that it applies bear directly on competition among re-users. The case of the mortgage and land-registry data held by the *Agenzia delle entrate* (Italian Revenue Agency) illustrates this: data collected for institutional purposes which constitute, at the same time, the essential *input* of value-added private information services.[35]

European case law has moreover excluded that the activity of collecting and making data available in a public register constitutes an economic activity for the purposes of the application of the competition rules, with the effect of removing from antitrust law conduct that nonetheless stands on the markets for derived information.[36]

The data is thus confirmed as being at once a resource of administrative action and, together, an economically significant and contested asset, without the legal order having fully regulated the balance between the two perspectives.

D. The protection of personal data in administrative action

For the protection of personal data too, the adaptation of the Italian legal order to European law took place through d.lgs. 101/2018, which did not replace the *Codice in materia di protezione dei dati personali* (Personal Data Protection Code) enacted by d.lgs. 196/2003, but amended it so as to adapt it to Regulation (EU) 2016/679, which now traces the general framework of reference, while the Code governs the aspects left to the rules of the national legal order.[37]

The point of greatest significance of d.lgs. 196/2003 for administrative action is the le-

34 On the relationship between the various regimes of openness, see Falcone, M., *Dati aperti e diritto al riutilizzo delle informazioni: la declinazione italiana del paradigma degli open data*, cited above; Carloni, E., *L'amministrazione aperta. Regole strumenti limiti dell'open government*, cited above. On the qualification of the silence kept on an application for the re-use of documents containing public data under Art 5 of d.lgs. 36/2006—classified as silence-failure-to-act, distinct from the silence-rejection proper to documentary access—see Consiglio di Stato (Council of State), Sec. III, 2 April 2025, no. 2818, with a note by Sola, A., *Il riutilizzo dei dati pubblici: quale tipologia di accesso amministrativo?*, in *Giornale di diritto amministrativo*, 2026, no. 1.

35 See Gaspari, F., *L'agenda digitale europea e il riutilizzo dell'informazione del settore pubblico. Il riutilizzo dei dati ipotecari e catastali*, cited above.

36 CJEU, 12 July 2012, Case C-138/11, *Compass-Datenbank GmbH v Republik Österreich*, concerning the database of the Austrian companies register.

37 D.lgs. of 10 Aug. 2018, no. 101, laying down provisions for the adaptation of national legislation to the provisions of Regulation (EU) 2016/679.

gal basis of public processing (Article 2-ter). In the original 2018 structure, the legal basis required by Article 6(3)(b) of the Regulation consisted exclusively of a provision of statute or, in the cases provided for by statute, of regulation: a reservation that made formal legality the safeguard of public processing.

D.l. 139/2021, converted into l. 205/2021, loosened this safeguard in two respects: it admitted that the legal basis might also consist of general administrative acts, and it established, by paragraph 1-bis, that processing by public administrations and by State-controlled public companies is always permitted where necessary for the performance of a task carried out in the public interest or for the exercise of official authority, the purpose being indicated, where not provided for by the legislation, by the controlling administration itself. The amendment, which took shape during the period of NRRP implementation, has a precise direction: to remove the formal obstacles to the circulation of data among administrations. The tension between protection and circulation was not, however, resolved by substantive criteria of balancing, but was settled by shifting the safeguard from formal legality to the responsibility of the controller.[38]

The rules are not, moreover, exhausted in Article 2-ter. For processing concerning special categories of personal data, Article 2-sexies requires that the processing be supported by a reason of substantial public interest and that the relevant legal basis (of Union law, of statute, of regulation or of a general administrative act) specify the types of data that may be processed, the operations that may be carried out, the reason of substantial public interest and the appropriate and specific measures to safeguard the fundamental rights of the data subject. For genetic, biometric and health-related data, Article 2-septies then comes into play, entrusting to the *Garante* the adoption of safeguard measures, while for data relating to criminal convictions and offences Article 2-octies applies.

There results a framework in which the general rules on public processing are articulated according to differentiated levels of intensity, depending on the nature of the data processed, but without this translating into a unitary body of rules governing public information assets.

Consistent with this evolution is the regime governing the communication of personal data among administrations: previously subject to a provision of statute or regulation, with a mechanism of prior consultation with the *Garante*, it is today permitted as a general matter where necessary for the performance of tasks of public interest, with a residual prior notice to the authority in those cases in which the legal basis lies in a general administrative act. The balancing is thus carried out case by case, on the part of the controlling administration, while the *Garante* retains advisory, corrective and sanctioning powers, exercisable also vis-à-vis public bodies, under a regime of case-by-case, ex post review.

To each European logic the Italian legal order has thus responded with a dedicated instrument: to the paradigm of data-as-infrastructure with the National Digital Data Platform, to that of circulation with d.lgs. 36/2006, to that of protection with the amended Code; and each response has operated by amending pre-existing provisions, without any overall revision of the regulatory structure.

38 Art 2-ter of d.lgs. 196/2003, introduced by d.lgs. 101/2018, was amended by Art 9 of d.l. 139/2021, converted by Law of 3 Dec. 2021, no. 205. On the loosening of the standard of legality that resulted, see Ponti, B., *Attività amministrativa e trattamento dei dati personali. Gli standard di legalità tra tutela e funzionalità*, 2023, Milan, FrancoAngeli, especially p. 103 ff.

The requirement of protection, which by its nature runs through all the other rules on public data, has therefore been progressively adapted to the needs of circulation and interoperability, including through the attenuation of earlier safeguards of formal legality and prior control.

This has not, however, led to the construction of a unitary framework of balancing between the protection, availability and re-use of the data, but has rather transferred onto the controlling administration the responsibility of reconciling, case by case, different interests and legal regimes. It is precisely here that one of the most problematic features of the national system emerges: fragmentation concerns not only the plurality of sources, but also the distribution of decision-making responsibilities among the legislature, the controlling administration, the supervisory authority and re-users.

IV. Sectoral profiles: data in healthcare and in land governance

It is, moreover, in the individual sectors that data makes its weight felt in administrative action. Among these, two fields appear particularly illustrative. Healthcare, where one finds both the data most sensitive for the person and, together, the most advanced European infrastructures, with the first sectoral data space of a binding character (see above, II.C).[39] But also land governance, because in it the dual nature of the public data emerges: a cognitive infrastructure of the decision and, ever more frequently, a yardstick to which the decision itself is anchored.[40]

In healthcare, the central instrument is the *fascicolo sanitario elettronico* (electronic health record), established by Article 12 of d.l. 179/2012:[41] a collection of digital health and social-health data and documents referring to the patient, populated by those who care for the patient and given novel incentive by the NRRP investments. The record is created for care purposes, but the provision assigns to it from the outset also purposes of study and scientific research and of healthcare planning, verification and assessment. Thus, within a single instrument, different purposes coexist, which the general rules keep distinct, with their respective regimes. Since these are special categories of data (the object of Article 9 of the Regulation), the processing further passes through the conditions of Article 2-sexies of the privacy Code and through constant consultation with the *Garante*. Onto this arrangement the European Health Data Space is now inserted, which requires the record to be coordinated with the European architecture of primary and secondary

39 On data in the health administration, see Falcone, M., *Le potenzialità conoscitive dei dati amministrativi nell'era della «rivoluzione dei dati»: il caso delle politiche di eradicazione dell'epatite C*, in *Istituzioni del Federalismo*, 2017, no. 2, p. 421 ff.

40 See Demichelis, M., *Territorio digitale per una buona amministrazione*, in *CERIDAP*, 2025, no. 4, on the interoperability of territorial data and on integration towards the common European data space, as well as id., *Il governo digitale del territorio. Dagli usi temporanei alla rigenerazione urbana*, 2023, Naples, Jovene.

41 Art 12 of d.l. 179/2012, converted, with amendments, by l. 221/2012. The provision assigns to the record purposes of prevention, diagnosis, treatment and rehabilitation; of study and scientific research in the medical, biomedical and epidemiological fields; and of healthcare planning, verification of the quality of care and assessment of healthcare assistance.

use: the sector in which the data is most protected is thus also the one in which the pressure towards circulation is most intense, and the reconciliation of the two requirements is entrusted to a stratification of sources—domestic, regional and European—that reproduces, on a smaller scale, the general framework.

In land governance, the data operates first of all as a cognitive infrastructure. Directive 2007/2/EC imposed the construction of an infrastructure for spatial information founded on metadata and interoperable services, transposed by d.lgs. 32/2010; the national repertory of territorial data, already encountered among the databases of national interest (see above, III.A), constitutes its national access point.[42]

The data then enters the administrative procedure, and it is in particular the regional laws on land governance that found planning upon formalised cognitive frameworks, which condition the lawfulness of the choices.

And it finally becomes a parameter of the decision, as shown by the monitoring of land take, the results of which, in the absence of a State framework law of principles, are taken up by regional laws as a reference for objectives and limits of transformation. Here, inevitably, fragmentation also takes on a territorial dimension, since regional information systems have developed heterogeneously, and the uniformity that State informational coordination may impose (see above, III.B) stops where regional competences begin.

The two sectors thus confirm how data is everywhere a resource of action, but the rules that govern it accumulate (general and special, State, regional and European) in the absence of a coherent and clear framework of reference and without criteria of coordination.

The two fields considered confirm, from different perspectives, the same critical point. In healthcare the tension arises between the protection of personal data, secondary use and European interoperability; in land governance, between the quality of the data, technical standardisation and its shaping influence on the administrative decision. In both cases, the data is no longer a mere cognitive precondition of public action, but becomes a structural element of the administrative function, without the legal order yet having categories fully adequate to govern its production, circulation and the attendant responsibility.

And it is upon this fragmented framework that the administration is today required to implement algorithmic tools, and where the structural weaknesses of the system may also have a significant impact.

V. Structural weaknesses of the national system

Beyond the absence of a unitary design of the rules that govern the data, there are further weaknesses that affect the data-governance system.

The first concerns the organisational aspect. The stratification of sources is matched by a multiplication of the actors responsible for governing data: political direction at the Presidency of the Council, technical rules and supervision in the hands of AgID, security

42 Directive 2007/2/EC of 14 March 2007 establishing an Infrastructure for Spatial Information in the European Community (INSPIRE), transposed by d.lgs. 32/2010. The national repertory of territorial data is regulated by Art 59 CAD; the relevant guidelines were adopted by AgID with determination no. 50/2022.

at the *Agenzia per la cybersicurezza nazionale* (National Cybersecurity Agency), the protection of personal data at the *Garante*, in addition to the individual controlling administrations and the operators of the platforms. Each legislative measure has conferred new functions without establishing a centre of coordination of the public information function, which thus remains divided by aspect (technical, security, protection).

It follows that administrations continue to manage their own information assets according to siloed logics, and adherence to the common infrastructures has had to be supported by prescriptive and incentivising mechanisms, to the point of linking the failure to comply with the obligations to make data available to the performance-related remuneration of senior managers (see above, III.B).[43]

The episode of the National Data Strategy, already observed (see above, III.A), illustrates this: the legal order realised the instrument, namely the National Digital Data Platform, without however first giving itself an orientation.

Fragmentation has, finally, a vertical dimension: regional and local information systems have developed heterogeneously, and State informational coordination, although founded on Article 117, second paragraph, point (r), of the Constitution, has been exercised more through platforms and specific obligations than as a stable function of governing the data.

The second weakness concerns the capacity of administrations to exercise in practice the functions that the rules on data assign to them. The provisions examined presuppose, in fact, structures capable of collecting quality data, classifying them, preserving them and rendering them interoperable and re-usable: they presuppose, that is, a function of governing the data that requires dedicated technical, legal and organisational skills. Here too the principle of adequacy applies, which requires a correspondence between the complexity of the function and the organisational suitability of the body called upon to perform it:[44] if the function consists in governing the public information assets, the administration must have the necessary structures and professional skills, and this suitability ought to be ascertained in advance, in accordance with an indication already present in the legislation on the conferral of functions.[45]

Yet reality appears, to a certain extent, still distant from this benchmark. Data-related skills (from data science to the management of quality and interoperability) remain scarce,[46] and the organisational safeguard that should ensure them, the Digital Transition Officer together with the relevant office, has in many cases resolved into a nominal des-

43 On the management of information assets according to 'siloed' logics, see Carloni, E., *Algoritmi su carta. Politiche di digitalizzazione e trasformazione digitale delle amministrazioni*, cited above; on the coordination of the information function in administrative pluralism, Merloni, F., *Coordinamento e governo dei dati nel pluralismo amministrativo*, cited above.

44 Cf. Cavallo Perin, R., *L'organizzazione delle pubbliche amministrazioni e l'integrazione europea*, in Ferrara, L., Sorace, D. (dir.), *A 150 anni dall'unificazione amministrativa italiana*, vol. I, 2016, Florence, FUP, p. 10; Carloni, E., Cortese, F., *Diritto delle autonomie territoriali*, 2020, Milan, Wolters Kluwer, p. 85 ff.

45 Art 4, para 3, point (g), of Law of 15 March 1997, no. 59. On the point, see Racca, G.M., Ponzio, S., *La scelta del contraente come funzione pubblica: i modelli organizzativi per l'aggregazione dei contratti pubblici*, in *Dir. amm.*, 2019, p. 38.

46 Cf. Falcone, M., *La data science come nuovo sapere per governare le intelligenze artificiali nelle pubbliche amministrazioni*, in *Riv. it. inf. dir.*, 2024, no. 2, p. 531.

ignation, devoid of resources and of any real capacity for direction.[47]

The gap is then accentuated by the size of the bodies: what a ministry or a large region can oversee with dedicated structures remains beyond the reach of the great majority of municipalities, without the associative forms provided for by the legal order having so far bridged the distance.

The consequence is that outsourcing becomes the ordinary solution: the administration that does not know how to process its own data entrusts their management to private operators, that is, to the market. The choice is often unavoidable, but it is not neutral. Recourse to the supplier cannot translate into a delegation of the governance of data: the quality, integrity and availability of information assets remain public functions, and the body must retain the capacity to define the requirements, verify the results and resume control of its own data at the end of the relationship. Where this capacity is lacking, outsourcing turns into dependence, an aspect to which we shall return immediately below.[48]

The legislature shows that it is aware of the problem, but appears unwilling to address it fully. Article 14 of l. 132/2025, in requiring administrations to adopt technical, organisational and training measures for the use of artificial intelligence, specifies that this is to be provided for with the resources available under existing legislation. The financial-invariance clause, customary as it is, here touches the heart of the problem: new capacities are not built at zero cost, and an organisational obligation devoid of resources risks being reduced to a formal fulfilment.[49]

The third critical aspect concerns the place, both material and legal, in which public data reside.

They are increasingly stored and processed through infrastructures and services provided by private operators according to 'as a service' models, in which the administration does not control the infrastructure and often not even the formats and the conditions of access to its own data.

There results a risk of *lock-in* that bears directly on the function: information assets that cannot be migrated, re-used or returned are assets that are public only in name. The push towards migration is, moreover, an explicit orientation: the cloud-first principle requires administrations to consider cloud solutions as a matter of priority, and the *Strategia Cloud Italia* (Cloud Italy Strategy) has made it a national programme.[50]

47 Cf. De Donno, M., *Le pubbliche amministrazioni come ecosistemi digitali. Regole e prassi di una trasformazione organizzativa*, in Gardini, G., Ricci, A., Ferrara, M.D., De Donno, M. (eds.), *Nuove tecnologie per nuove amministrazioni*, 2025, Turin, Giappichelli, p. 41 ff., especially pp. 55-57.

48 Reference may be permitted to Rosa Salva, P.M., *The adequacy of the procurement function between digital transition and cybersecurity: the necessary qualification and specialisation of contracting authorities*, in *Ius Publicum Network Review*, 2022, no. 1, pp. 1-36. On the position of the supplier, cf. Ponti, B., *Il fornitore dell'algoritmo quale soggetto estraneo all'amministrazione*, in *Rivista italiana di informatica e diritto*, 2024, no. 2.

49 Art 14, paras 3 and 4, of l. 132/2025. Paragraph 4 specifies in particular that administrations are to provide for this 'with the human, instrumental and financial resources available under existing legislation'.

50 The cloud-first principle is enunciated among the principles of the Three-Year Plan for Information Technology in Public Administration; the *Strategia Cloud Italia* (Cloud Italy Strategy), defined in September 2021 by the Department for Digital Transformation and the National Cybersecurity Agency, made it a national programme, placing among its objectives technological autonomy, control over data and the resilience of digital services. It finds its legislative foundation in Art 33-septies of d.l. 179/2012 (converted by l. 221/2012), as replaced by Art 35 of d.l. 76/2020 (converted by l. 120/2020) and subsequently amended, which—for the declared purpose of protecting the country's technological autonomy—

The system of qualification of cloud services for the public administration, now embedded within the National Cybersecurity Agency,[51] safeguards first of all the security aspects, but does not by itself close that of dependence, which needs to be governed already at the contractual stage, through conditions of portability, reversibility and technological autonomy of the public party.[52]

These three weaknesses may then converge, posing fundamental challenges to the public administration, for example when the data becomes the *input* of artificial-intelligence systems.

Here the quality of the data ceases to be an objective of good administration and becomes a condition of the lawfulness of the action, since the results of the system, and therefore the very decisions that derive from it, depend on the accuracy and representativeness of the training data.[53]

It is precisely this aspect that reveals the problematic features of the present system, where fragmentation translates into databases that are incomplete and often non-communicating. Furthermore, the deficit of capacity prevents the administration from verifying the data employed and the *outputs* produced. And technological dependence then transfers to the supplier decisions that bear on the function.

This is a system that does not guarantee the quality and interoperability of its own data, and that consequently cannot guarantee the lawfulness of the algorithms that use them. The legislature itself, for that matter, has acknowledged the absence of comprehensive rules on the subject, delegating to the Government, by Article 16 of l. 132/2025, the power to define them as regards the use of data, algorithms and mathematical methods for the training of artificial-intelligence systems. It is confirmation that the governance of the data constitutes the precondition (today for the most part lacking) of algorithmic administration, and the point from which the prospects for reform must move, as will be discussed.[54]

requires public administrations to migrate their data and digital services towards the National Strategic Hub, towards digital infrastructures meeting the prescribed requirements, or towards qualified cloud services, referring to a regulation the classification of data and services, the minimum levels and the arrangements for migration and qualification (on which see immediately below).

51 The ordinary regime of qualification of cloud infrastructures and services for the public administration is entrusted to the National Cybersecurity Agency; the relevant regulation was adopted by directorial decree A.C.N. no. 21007/24 of 27 June 2024, applicable from 1 Aug. 2024.

52 Cf. the draft AgID Guidelines on the procurement of artificial-intelligence systems in the public administration, whose consultation process was launched by determination no. 43 of 10 March 2026, especially § 3.4, where the data is qualified as a public *asset* to be considered from the very planning of the award, with the provision of requirements on the accuracy, traceability and updating of data and of clauses on access, portability and return at the end of the relationship.

53 Cf. Cavallo Perin, R., *Ragionando come se la digitalizzazione fosse data*, in *Dir. amm.*, 2020, p. 326. In the case law, on the requirements of data quality and of knowability of the logic used, see Consiglio di Stato (Council of State), Sec. VI, 8 April 2019, no. 2270, and Sec. VI, 13 Dec. 2019, no. 8472.

54 Art 16 of l. 132/2025, introduced, moreover, in the course of the parliamentary examination (Art 14-bis of Senate Bill no. 1146-A). The delegation, to be exercised within 12 months, has as its object comprehensive rules on the use of data, algorithms and mathematical methods for the training of artificial-intelligence systems, without further obligations, in the fields subject to Regulation (EU) 2024/1689, beyond what is already laid down therein.

VI. Prospects for reform: towards data administration

If the data is destined to become ever more central in public action, the action of the administration (which is carried out on the basis of data and, at the same time, for the management of those very data) still lacks a complete and adequately structured body of governing rules. Of this the legislature itself appears aware, having opened two regulatory reform projects almost simultaneously. On the one hand, by the law on artificial intelligence, the Government was delegated to define comprehensive rules on the use of data, algorithms and mathematical methods for the training of systems.[55] On the other, the annual simplification law likewise delegated the simplification, amendment and integration of the Digital Administration Code, expressly with a view to valorising and strengthening public information assets.[56]

The two delegations, however commendable, do not however set out criteria fully consistent with the problems to be addressed. In particular, the guiding criteria of Article 16 orient the rules on the training of systems towards the rights and obligations of the party intending to use the data, the instruments of compensatory and injunctive protection and the jurisdiction of the specialised business divisions: data is there considered as an object of relationships and of litigation, rather than as a resource of an administrative function. Article 11, for its part, after invoking public information assets, breaks it down into two criteria (the updating of electronic identity and trust services and the strengthening of interoperability through the National Digital Data Platform) which assume specific legal mechanisms without redefining the governance of data as such. The horizon remains that of targeted measures built upon the existing framework, rather than its strengthening.[57]

A not dissimilar approach may, for that matter, be discerned on the European side. With the Digital Omnibus the Commission has set in motion a consolidation of part of the rules on data—the repeal of the open data directive, the Data Governance Act and the regulation on the free flow of non-personal data, whose rules would be merged into a restructured Data Act (see above, II.E)—justifying it by the need to reduce the overlaps that the accumulation of rules has produced. Here too, however, these are targeted amendments and selective repeals which do not aim at a comprehensive consolidation of the regulatory framework on data.

55 The delegation, under the aforementioned Art 16 of l. 132/2025, is oriented by the guiding criteria of para 3, which concern the legal regime of the use of data and the rights and obligations of the party intending to proceed with such use (point (a)), the instruments of compensatory and injunctive protection and the sanctioning apparatus (point (b)) and the assignment of the relevant disputes to the specialised business divisions (point (c)); the draft decrees are adopted on the proposal of the President of the Council of Ministers and of the Minister of Justice.

56 The delegation, provided for by Art 11 of l. 167/2025, is avowedly aimed at 'valorising and strengthening the public information estate, the processes of digitalisation of public administrations and the delivery of online services', but the guiding criteria of para 2 are limited to the updating of the means of electronic identification and of trust services (point (a)) and to the strengthening of the interoperability of systems and databases through the National Digital Data Platform (point (b)).

57 On the incremental and sectoral character of the rules, in the absence of a general design, and on the organisational resistance to innovation, see D'Orlando, E., Orsoni, G., *La digitalizzazione e l'organizzazione della pubblica amministrazione*, editorial, in *Istituzioni del Federalismo*, 2023, no. 2, p. 279 ff.; Torchia, L., *Pubblica amministrazione e transizione digitale*, in *Giornale di diritto amministrativo*, 2024, no. 6, p. 729 ff.

It is here, instead, that reform at the national level could make a difference. The weaknesses identified—fragmentation, lack of capacity, dependence—are not corrected by multiplying sectoral sets of rules, but by recognising a function in its own right in the administration of data, endowed with its own organisation, with defined responsibilities and with adequate resources.

The revision of the CAD ought therefore not to confine itself to rationalising platforms, digital identities and services, but to assume public information assets as an autonomous object of regulation. This implies common rules on the quality, ownership, updating, interoperability and traceability of data, on the responsibility for making them available, and on the relations between openness, protection and algorithmic use. Only in this perspective can the data be governed not as a by-product of digital administrative activity, but as an infrastructure of the public function.

In this direction lie at least three requirements. A coordination of the public information assets, capable of bringing together what is today divided between direction, technical rules, security and protection.[58] An effective organisational safeguard within the individual administrations—for example the Digital Transition Officer and its office—no longer nominal, but endowed with skills and means.[59] And the coordination between the governance of data and migration towards the cloud: the cloud-first principle and the Cloud Italy Strategy place among their objectives control over data and technological autonomy, which however remain entrusted to the capacity of the public party to govern the relationship with the supplier in terms of portability and reversibility, so that migration does not turn into dependence.[60]

Upon all these aspects weighs the question of resources. Organisational obligations continue to be accompanied by financial-invariance clauses, but a function without means remains on paper, and no reform of data governance can dispense with the investment in skills and structures that it presupposes.[61]

All of this holds, moreover, inasmuch as the shift accomplished by European Union law and by its logics—in particular from the protected data to the data as infrastructure and resource, including for public action—is realised not by legislative means but through organisation: where the administration does not equip itself to administer data, and not merely to make use of them, the change of paradigm risks remaining on paper (even if digitalised).

58 On the function of IT coordination and on the dispersion of competences among administrations, Torchia, L., op. cit.; Merloni, F., *Coordinamento e governo dei dati nel pluralismo amministrativo*, cited above.

59 On the Digital Transition Officer as an organisational safeguard and on the deficit of skills, De Donno, M., op. cit.; Falcone, M., *La data science come nuovo sapere per governare le intelligenze artificiali nelle pubbliche amministrazioni*, cited above.

60 On cloud-first and on the Cloud Italy Strategy, see above, in particular note 50. Control over data and technological autonomy, among the declared objectives of the Strategy, presuppose that the public party govern the relationship with the supplier in terms of portability and reversibility, including at the stage of qualification of cloud services before the National Cybersecurity Agency (see again above, Section V).

61 Art 23 of l. 167/2025, laying down the financial-invariance clause; similarly, for the obligations of administrations concerning artificial intelligence, Art 14, para 4, of l. 132/2025.