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

Data and public administration

Laszlo Van Daal
Ph.D. candidate, Université Paris 1 Panthéon-Sorbonne (IRJS)
Teaching assistant, Université Rennes 2
Scientific assistant, Saarland University

Abstract:

This article examines the relationship between data and public administration. At first glance, the subject might appear to be a matter of government transparency and open data alone; in fact, it reaches considerably further. Public administration lies at the heart of the data economy, which it organizes as much as it takes part in. Far from being confined to public-sector data, it governs both the flow of private data and the protection of personal data. The stakes are as broad as they are varied, spanning the pursuit of the public interest, the stimulation of the market, and the safeguarding of privacy. To reconcile them, public administration commands a range of instruments and techniques designed to strike the best possible balance. Yet the very nature of the data economy exceeds the reach of any single national administration. In the age of artificial intelligence, the equilibria that once prevailed are being disrupted, reshaping the very challenges that public administration must now confront.

Keywords:

Administrative law, Data economy, Economic regulation, Circulation of data, Protection of data, European data law, Digital Sovereignty

---

'Grounding action upon large quantities of data is nothing new for administrations, once one considers their history. States, much like local institutions, have for centuries amassed enormous quantities of information of every kind'.[1]

---

1 Auby, J-B., "Le droit administratif face aux défis du numérique", *AJDA* 2018, p. 835.

Public administrations hold considerable stocks of data, amassed over the course of several centuries. As Jacques Chevallier and Lucie Cluzel-Metayer observe, until recent times public data 'were not regarded as such, but rather as resources mobilised by the State for the purposes of its functioning, embedded within a broader decision-making process into which they were absorbed'.[2]

As modern States took shape, data collection represented a decisional resource that underpinned public action and made it more effective, or at the very least more rational. The earliest systematic censuses for fiscal purposes thus date back from the Middle Ages,[3] and they undeniably contributed to consolidating the financial power of the State. Likewise, in a more recent period, the collection of geological data supported public works policies. The expansion of State activities under the welfare State diversified the nature of the data collected, extending it into the economic and social fields. Procedures for the collection and processing of data in the public sector were thereby refined, notably through the keeping of registers, cadastres and statistical instruments used by the administration.

From the late 1990s onwards, the generalisation of information technology enriched the volumes of available data, giving rise to new paradigms. On the one hand, the exploitation of public data formed part of the broader strategy of the *platform-State*.[4] On the other hand, the leading digital platforms seized upon the competitive advantage represented by the extraction and processing of data flows. By centralising large volumes of data and swiftly turning them to account, these actors acquired a dominant position, becoming indispensable to every other stakeholder on the market[5]—a development that calls upon the State to respond with appropriate economic regulation through public administration.

From a legal standpoint (and this concerns the public sector in particular), technological advances have been accompanied by an ever greater demand for transparency of administrative action,[6] expressed concretely through measures to facilitate the transmission and circulation of data.[7] Since the stakes involved are at once economic and tied to the preservation of certain liberties, the role of public administration (the State, the terri-

2 Chevallier, J., Cluzel-Metayer, L., "Les données publiques", *RFAP* 2018, n° 167, Introduction, p. 463.

3 Auby, J-B., "Algorithmes et Smart Cities : Données Juridiques", Contribution to the colloquium "Les algorithmes publics" ("Public Algorithms") held on 12 and 13 April 2018 at the University of Lorraine (Metz): Revue générale du droit online 2018, n° 29878. Available at: www.revuegeneraledudroit.eu/?p=29878.

4 Chevallier, J., "Vers l'État-plateforme ?" *Les données publiques*, *RFAP* 2018, n°167, p. 629.

5 Marty, F., "Économie de la donnée : Écosystèmes numériques, algorithmes et intelligence artificielle" in *L'émergence d'un droit des données*, 2023, p. 25.

6 Orofino, A. G., "Ouverture des données publiques et transparence de l'action administrative", in Lanna, M., (dir.), *Smart city et prise de décision*, 2023, Mare & Martin, pp. 37–45.

7 See: *Loi n°78-17 du 6 janvier 1978 sur l'informatique et les libertés*, JO (Official Journal of the French Republic), 7 Jan. 1978, p. 227; *Loi n°78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public*, JO, 18 July 1978, p. 2861; *Ordonnance n°2005-650 du 6 juin 2005 relative à la liberté d'accès aux documents administratifs*, JO, 5 June 2005, text n°13; *Loi n°2016-1321 pour une République Numérique du 7 octobre 2016*, JO, 8 Oct. 2016, text n°1.

torial authorities[8] and the regulatory authorities[9]) is best examined through an economic lens, and more precisely through its position on the market.

Public administration thus stands at the intersection of two logics, corresponding to the three positions it may occupy within the economy:[10] a *public-service logic*, under which it acts both as a *supplier* of data (whether on a paid or gratuitous basis) and as a *user* of data for general-interest purposes (the *prescriptive* State); and a *market logic*, under which it intervenes by virtue of its regulatory missions, outside the market (the *regulatory* State), or within the market as a purchaser of data (the *collaborative* State).

'Data' and 'public administration' entertain multiple relations, according to the nature of the data under consideration and the position of the administration within the economy. First, public administration, as the holder of large volumes of data, will be encouraged to disseminate them actively—a task answering a democratic imperative (the demand for transparency of public action) as much as an economic one. With regards to the latter, it is presumed that the release of public data necessarily drives economic growth,[11] without considering the negative externalities borne by operators, both private

8 Under French law, *collectivités territoriales* (territorial authorities) are the constitutionally independent levels of local government. There are three principal types: *régions*, *départements* and *communes* (regions, departments and municipalities).

9 Under French law, *autorités de régulation* (regulatory authorities) are administrative bodies exercising supervisory and advisory functions across various economic sectors. Their distinguishing feature is a special status guaranteeing a degree of independence. Two categories exist: *autorités publiques indépendantes* (API), which possess legal personality as a public body, their strongest guarantee of independence; and *autorités administratives indépendantes* (AAI), which lack such legal personality and consequently enjoy not full independence but a high degree of autonomy.

10 Nicinski, S., "Droit public des affaires", Précis Domat, 8th edn., LGDJ, §3 – p. 19, according to our translation: 'The three positions of the administration: first, the State may intervene as a public authority to regulate, influence, steer, direct or protect the market and its economic operators. It administers the economy and appears as an authority external to the market, upon which it imposes its will. Second, the State itself acts as a supplier of goods and services on the market, whether by reason of a public service, the presence of historically established public operators, or simply to acquire resources. Third, the State may cooperate with economic operators, either to meet its own needs or, more indirectly, to fulfil a general-interest objective for the benefit of the population; in this capacity it occupies the position of a demand-side actor. From these three situations emerge three figures of the State: the regulator (or 'prescriber State'), the economic operator, and the collaborator with economic operators.'

11 'The objective pursued [of making public data free of charge] is to foster innovation and economic development through the free and unrestricted reuse of substantial data resources', according to our translation of Sauvé, J-M., Opening of the colloquium "La valorisation économique des propriétés des personnes publiques", Colloquium organised by the Conseil d'État on 6 July 2011 at the École nationale d'administration (Paris), p. 16. This approach has been widely adopted in the conception of open data in France following the report "Ouverture des données publiques – Les exceptions au principe de gratuité sont-elles toutes légitimes" submitted by M. Mohammed Adnène Trojette to the Prime Minister in July 2013. Moreover, this approach was given legislative recognition in the '*Loi pour une République numérique*'. The impact study of that law stated (according to our translation): 'This proposal aims to increase the volume of administrative documents made available online by public authorities under the open data policy, in order to enhance the transparency of public authorities, improve public services, and stimulate the development of new economic activities' (See impacts study on the proposal of *loi pour une République numérique,* 9 December 2015 p. 14). To date, no academic study has quantitatively demonstrated the ability of French private economic operators to generate economic value from these public data over the past decade. Moreover, the answer can only be deemed satisfactory if it is demonstrated that the valorisation of public data by the public sector is sufficiently significant

and public, subject to the overwhelming market power of *BigTech*. Yet public administration may equally facilitate the dissemination of certain data, just as it is called upon to guarantee the protection of others. The notion of public administration is itself a broad one, encompassing territorial authorities, regulatory authorities, the State and even the European institutions, across a spectrum ranging from the smallest *commune* to the European Union.

Beyond its various forms, public administration must also be examined in terms of how, through its law-enforcement, regulatory and public-service functions, it pursues the general interest—with varying degrees of success—against the backdrop of an increasingly complex body of data-related legal rules and the ever-broader scope of the interests at stake.

The European Union has developed a body of data law structured around objectives that are diverse, at times cross-cutting and occasionally competing. These aim to: promote the release of data, whether by organising the conditions under which public bodies make theirs available (Open Data Directive[12]) or by orchestrating the circulation and use of data regardless of their nature (Data Governance Act[13]); correct market imbalances by regulating conditions of access and use among economic actors (Data Act[14]) or by governing the conduct of access controllers, the 'gatekeepers' (Digital Markets Act[15]); and govern the free movement of data, whether personal (General Data Protection Regulation[16]) or non-personal (Regulation on the free flow of non-personal data).[17]

This normative corpus forms the legal infrastructure of 'the European data strategy'[18],

to justify the abolition of the fees in this area that this approach has entailed. The fee previously constituted the main source of income for local authorities to implement the public service of data and to finance the infrastructure and expertise essential to it. Consequently, the public service of data at local level (also referred to as the 'local public service of data' or the 'territorial public service of data') do not have the resources to develop.

Finally, it should be noted that, due to its counterproductive effects on open data policies, the principle of free access to data could be undermined by the 'Digital Omnibus' regulation proposal, which could introduce a fee for 'very large enterprises,' effectively targeting the Big Tech firms first and foremost.

12 Directive (UE) 2019/1024 Of the European Parliament and of the Council, of 20 June 2019 on open data and the re-use of public sector information (recast), OJEU L 172 of 26 June 2019, pp. 56-83.

13 Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance), OJEU L 152 of 3 June 2022, pp. 1-44.

14 Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) (Text with EEA relevance), OJEU L 352 of 22 Dec. 2023, pp. 1-44.

15 Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance), OJEU L 265 of 12 Oct. 2022, pp. 1-66.

16 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJEU L 119 of 4 May 2016, pp. 1-88.

17 Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Text with EEA relevance), OJEU L 303 of 28 Nov. 2018, pp. 59-68.

18 Communication from the Commission to the European Parliament, the Council, the European Economic and Social

casting new light on the notion of 'data' through the prism of administrative law, and of administrative action in particular. The administration is no longer confined to the role of producer of public data; it is now called upon to act as a user of data originating from private persons, whether legal or natural. The conceptual framework shifts accordingly. Where the administration once operated within the familiar domain of public information, it must now come to terms not only with the digitisation of that information but also with the diverse legal categories the notion of data may encompass.

In technical terms, a unit of digital data is defined as 'an elementary digital representation, in coded form, of an entity (thing, event, measurement, transaction, etc.) intended to be collected, recorded, processed, manipulated, transformed, preserved, archived, exchanged, disseminated, communicated'.[19] As a legal object, however, the notion is less straightforward. The law does not always employ the term 'data', at times preferring formulations that refer to legal objects of broader or more established scope. Data may differ in nature, each calling for its own definition—definitions that may converge, complement or intertwine with one another. Some data benefit from a clear legal definition; others do not. And where definitions are provided by a text, they may be particularly laconic: to the benefit of broader application, certainly, but to the detriment of precisely defined limits.

The latest European regulations all share the same definition of data within their respective Article 2: 'any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audiovisual recording'.[20] An exhaustive account of the notion, however, requires attention to the differing forms data may assume: public data, private data, personal data and non-personal data.[21]

As regards 'public data', these are readily identifiable in French law under a broader designation: that of *documents administratifs* (administrative documents). Under Article L. 300-2 of the *Code des relations entre le public et l'administration* (Code on Relations between the Public and the Administration), public data are those 'produced or received in the performance of a public-service mission', for which the *loi pour une République numérique* (Law for a Digital Republic)[22] established an extensive regime of accessibility and re-use, enshrining a principle of openness by default. European law, for its part, aligns public

Committee and the Committee of the Regions, 'A European Strategy for Data', COM(2020) 66 final, 19 Feb. 2020.

19 Administrateur général des données (Chief Data Officer of french government), "Les données au service de la transformation de l'action publique", report to the Prime Minister on data governance, Dec. 2015, p. 16.

20 Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance), OJEU L 152 of 3 June 2022, pp. 1-44; Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 Sept. 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance), OJEU L 265 of 12 Oct. 2022, pp. 1-66; Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 Dec. 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) (Text with EEA relevance), OJEU L 352 of 22 Dec. 2023, pp. 1-44.

21 According to the various definitions set out in the communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A European strategy for data, 19 Feb. 2020.

22 *Loi n°2016-1321 pour une République Numérique du 7 octobre 2016*, JO, 8 Oct. 2016, text n°1.

data with a related notion: that of 'open data', defined as 'data in an open format that can be freely used, re-used and shared by anyone for any purpose'.[23] Such data are the object of policies that 'encourage the wide availability and re-use of public sector information for private or commercial purposes, with minimal or no legal, technical or financial constraints, and which promote the circulation of information not only for economic operators but primarily for the public'.[24]

The natural counterpart to public data would be private data. By extension, any data not qualifying as public are necessarily private,[25] a category that would encompass both personal data and the data of private legal persons. For present purposes, however, private data should be understood as data 'of the private sector'[26] or 'produced by private actors'[27] and in particular corporate data.[28] Given that the notion leans towards private legal persons, and that an *ad hoc* regime governs the data of natural persons, private data are associated with the information assets of companies, associations and other private organisations. Private data would thus be any data bearing neither the characteristics of public data nor those of personal data.

Personal data are more readily identifiable, since the GDPR defines them as 'any information relating to an identified or identifiable natural person'.[29] Here, digital data are assimilated to 'information' understood as 'an intangible, formalised and meaning-bearing entity'[30], a notion that the text does not appear to distinguish from that of data.[31] This definition is a relatively broad one, liable to give rise to '[issues] of delimitation and effectiveness'.[32]

The extensive material scope of the GDPR implies that the law of personal-data protection must be reconciled with the legal regimes governing other types of data, public data in particular.[33] The competing objectives pursued by these various regimes have

23 Recital n° 16 of directive (UE) 2019/1024 of the European Parliament and of the Council, of 20 June 2019 on open data and the re-use of public sector information (recast), OJEU L 172 of 26 June 2019, pp. 56-83.

24 Ibid.

25 Cassar, B., "Données - Gouvernance des données", *Répertoire IP/IT et Communication*, Dalloz, 2022 (See n°11).

26 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A European strategy for data, 19 Feb. 2020, p. 8-9.

27 Tifine, P., "Données privées d'intérêt général, Partage de données entre l'administration et le secteur privé", *JC. Adm.* 2024, Fasc. 109-90.

28 Database - Chapter 1: Economic Issues of Databases - Section 2: Evolution of Databases, Permanent Dictionary of Business Law (See n°6).

29 Article 4-1 of regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJEU L 119 of 4 May 2016, pp. 1-88.

30 "Qu'est-ce qu'une donnée personnelle ?", Protection des données personnelles – smart action EL, *Dalloz.fr. online* (consulted on 19 June 2026). Also available at: https://open.lefebvre-dalloz.fr/droit-affaires/protection-donnees-personnelles/donnee-personnelle_a93583.

31 Ibid.

32 Castets-Renard, C., "La protection des données personnelles dans les relations internes à l'Union européenne", *Répertoire de droit européen* 2018, n° 221.

33 Article 2-1 of regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and

compelled the search for 'a fair balance [...] between the pursuit of administrative transparency, grounded in the possibilities of re-use of released information, and the need to ensure compliance with the rules on personal-data protection'.[34]

In practice, data flows may comprise both personal and non-personal data; 'where the two types of data are inextricably linked, Regulation (EU) 2016/679 takes precedence by virtue of personal-data protection requirements'.[35]

The latest European regulations also share, in their respective Article 2, the definition of 'non-personal data' as any 'data other than personal data'. Like that of private data, the notion is at once inclusive and exclusionary: it sets aside personal data *de facto*, yet draws together all data whose free flow is promoted—certain private data of economic operators, industrial data, de-personalised or anonymised data[36]—as well as public data, whose openness by default and free re-use carry 'economic and social stakes of particular importance'.[37]

This taxonomy of the various legal meanings of the notion brings into view the dynamics of data circulation and the interests at play. Data are of interest to public authorities, but also to private operators whose capacity for innovation generally surpasses that of the State. *BigTech*, on the strength of the considerable volumes of data they hold and their capacity to exploit them, rival public services in their ability to ground decisions on an optimal informational basis. Google, for instance, holds data assets and technical means that could substantially facilitate the State's administrative action. The State's only recourse is to encourage and secure the circulation of data, beginning with access to and re-use of its own. Against this backdrop, the major platforms—data-hungry by nature—are reshaping the balance of power between public and private actors by generating their own normative frameworks, and raise serious concerns from the standpoint of competition.[38]

A regulatory impulse thus emerged, caught between 'the entanglement [...] of innovation and economic-development objectives'[39] and '[the] fears [...] that the unregulated release of data would benefit only the largest players in the digital economy, Google in particular, and undermine the business models of local companies'.[40]

In response, the State has turned to new mechanisms drawn largely from European law, in hopes of balancing these competing considerations.

The economic dimension is self-evident: among the vast quantity of data produced,

repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJEU L 119 of 4 May 2016, pp. 1-88.

34 Lanna, M., "Données publiques et protection des données personnelles : le cadre européen ?", *RFAP* 2018, n°167, p. 502.

35 Castets-Renard, C., *Droit du marché unique numérique et intelligence artificielle*, 2020, p. 318.

36 See: Favro, K., "Les données non personnelles : un nouvel objet juridique", *Dalloz IP/IT* 2020, p. 234; Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Building a European data economy, 10 Jan. 2017.

37 Favro, K., "Transformation numérique de l'administration", *Répertoire de service public*, Dalloz, 2023 (See n°26).

38 Marty, F., Teller, M., "Comment réguler l'IA ? L'inspiration du droit économique" in Castets-Renard, C. and Eynard, J. (dir.), *Un droit de l'intelligence artificielle : entre règles sectorielles et régime général,* 2023, Bruylant, p. 268.

39 Courmont, A., "Chapitre 5. Les licences : instruments centraux du gouvernement par les données" in *Quand la donnée arrive en ville : open data et gouvernance urbaine*, 2021, Presses universitaires de Grenoble, p. 101.

40 Ibid.

not all carry equal value in an open economy, and certain data are of strategic importance to public authorities and private operators alike. It thus falls to both to promote the circulation of data, an imperative rooted as much in European Union law as in national law. At present, however, the promotion of innovation and economic development benefits substantially from the circulation of public data into the private sector; the reverse flow—private data towards the public sector—remains insufficient. These economic considerations must in turn be reconciled with the imperative of preserving privacy and, more precisely, of protecting the personal data of those subject to administrative authority.

Such reconciliation is nothing new within the data economy or its handling by administrative law, yet the circulation of data now answers to the demands of a globalised economy that generates cross-border flows both within the European Union and beyond. The landscape is further transformed by heightened competition among the leading digital actors in the struggle for market dominance, and among States in the control of massive data volumes (*big data*).

A distinction must accordingly be drawn between two categories of data: non-personal data, for which free circulation is promoted while preserving a balanced market (I); and personal data, which remain within the principle of free movement but benefit from reinforced safeguards, a regime that sits at the heart of the data economy's sharpest tensions (II).

I. Non-personal data and public administration: free circulation as a democratic and economic objective

While the law of economic regulation provides the basic legal infrastructure for data circulation, with the contract as its preferred instrument, the position of certain actors who dominate the market points to a distortion of the balance of power; yet 'each must be able to derive advantage from the contract without any one party monopolising its fruits' (B).[41]

The latest European regulations on data seek to reorient this competitive market towards a new philosophy: *solidarism*.[42] Whether the aim is to 'guarantee the contestability and fairness of digital-sector markets within the Union' against the gatekeepers—the *GAFAM*—through the Digital Markets Act, or to encourage data sharing through intermediation via the Data Governance Act, a solidarist vision emerges from the European data strategy.[43] More than a deliberate choice of European law, this solidarism appears almost intrinsic, observable in the practices adopted by territorial authorities and in the action of certain regulatory authorities. The market is structured in such a way that smaller actors, almost instinctively, organise themselves—not out of purely commercial motives but with the shared aim of promoting data circulation—so as not to remain dependent on dominant players who have already seized the field (A).

41 Arcelin, L., "Solidarisme et concurrence : une (ré)conciliation sur le terrain du marché numérique" in Castets-Renard, C. and Eynard, J., (dir.), *Un droit de l'intelligence artificielle : entre règles sectorielles et régime général*, 2023, Bruylant, p. 302.

42 Ibid, p. 279.

43 Ibid, p. 282.

A. Multiple approaches, uncertain effects

In the modern economy, the free movement of goods, services and capital implies that the circulation of non-personal data within the EU must likewise be organised. The fragmentation of national regulations was, however, hindering the growth of digital enterprises. The Regulation on the free flow of non-personal data[44] sought to address this by establishing a digital single market, anticipating the creation of a single European data space[45] capable of structuring this economy.[46]

The Regulation aspired to enshrine a fifth freedom of movement, complementing those of goods, services, persons and capital, so as to strengthen European competitiveness; it suffered, however, from significant shortcomings.[47] Given the distinctive characteristics of data—inherently difficult to locate in a single place at a single moment—its provisions remained imprecise.[48] The Data Act of 2023[49] seeks to remedy these deficiencies by strengthening legal certainty for data consumers and producers, particularly in the field of the Internet of Things (IoT).[50] This requires, first, clearer rules on data use and, more importantly for present purposes, a commitment to facilitating the continuous transfer of data between holders and users. Yet while the Data Act emphasises free movement of data, such circulation may encounter resistance from producers (a public-service concessionaire, for instance) on account of the economic value certain data represent.[51] Against this background, public administration has proved particularly proactive in promoting data circulation, whether for purposes of transparency of public action (3), regulation (4), or economic development (2); these objectives at times converge (1).

1. The creation of a multiform 'public service of data'

Public administration has developed a number of responses building on the innovation introduced by Article 14 of the *Loi pour une République numérique* [Law for a Digital Republic], now codified at Article L. 321-4 of the *Code des relations entre le public et l'administration* [Code on Relations between the Public and the Administration], which instituted a public service of data at national level. This service is a State competence, operationally car-

44 Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Text with EEA relevance), OJEU L 303 of 28 Nov. 2018, p. 59-68.

45 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *A European strategy for data*, COM(2020) 66 final, 19 Feb. 2020, p. 5.

46 Recital n° 1 of Regulation (EU) 2018/1807 stating that: 'Electronic data are at the centre of those systems and can generate great value when analysed or combined with services and products'.

47 See: Benabou, L., "Une cinquième liberté de circulation numérique ? Est-ce possible ? Est-ce utile ?", *RTD eur.* 2021, p.279; Boev, I., "Le nouveau règlement : un 5e principe de libre circulation ?", *Dalloz IP/IT* 2020, p. 223.

48 Benabou, L. (2020), Une cinquième liberté de circulation numérique ? Est-ce possible ? Est-ce utile ?, op. cit., p. 224.

49 Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) (Text with EEA relevance), OJEU L 352 of 22 Dec. 2023, pp. 1-44.

50 Ibid, Recital n° 14.

51 Zolynski, C., "Un nouveau droit de propriété intellectuelle pour valoriser les données : le miroir aux alouettes ?", *Dalloz IP/IT* 2018, p. 94.

ried out by the *Etalab* unit within the *Direction interministérielle du numérique* [Inter-ministerial Directorate for Digital Affairs].[52] Although their role within this scheme remains undefined,[53] territorial authorities have equally sought to establish a public service of data at local level. A range of initiatives aimed at promoting data circulation have accordingly emerged. While all may be gathered under the banner of the 'local public service of data'[54] by virtue of their shared purpose, the means employed are eclectic.

Rennes Métropole, for instance, made the relatively uncommon choice of a dedicated service organised as a *régie* [directly managed public service], the *Service public métropolitain de la donnée* [Metropolitan Public Service of Data] (SPMD), tasked with carrying out 'general-interest missions relating to the production, circulation, use and sharing of data across the territory of *Rennes Métropole*'.[55] A product of its time and context, the SPMD incorporates RUDI (Rennes Urban Data Interface), a platform designed to 'promote the circulation of strategic data resources among territorial actors'.[56]

Others have turned, more unexpectedly, to a novel legal instrument for organising the local public service of data: the administrative charter. A number of *métropoles* have sought to govern the use and circulation of data within their territory by adopting a *charte métropolitaine des données* (metropolitan data charter), as in Nantes,[57] Brest,[58] Aix-Marseille-Provence[59] and Rueil-Malmaison.[60]

At first sight, these instruments invite scepticism as to their real reach, or, more pre-

52 Cluzel-Métayer, L., "La construction d'un service public de la donnée", *Revue française d'administration publique* 2018/3, n° 167, pp. 491-500.

53 Bécet, J.-M., "Communication des documents des collectivités territoriales au public : diffusion et réutilisation des données publiques", *Encyclopédie des collectivités locales*, Chapter 3, Nov. 2019, Dalloz, n° 12214.

54 See Hennion, C., Altounian, M., Monthubert, B., *Rapport de la mission Data et territoires*, Sept. 2023, p. 25; Fédération Nationale des Collectivités Concédantes et Régies, *Étude sur le cycle de la donnée dans la conception et la mise en œuvre des services et usages numériques des collectivités territoriales,* 2019, p. 107; Fédération Nationale des Collectivités Concédantes et Régies, *Collecte et gestion des données numériques pour le pilotage des politiques publiques : vers un big data territorial*, 2016, p. 79; Mazon, R., "Nous défendons un service public local de la donnée", *Gazette des communes*, 27 May 2019; Commission nationale du débat public, *Décision n° 2021/120/BREST GESTION DES DONNEES/1 du 1er septembre 2021 relative à l'avis méthodologique – Charte de gestion des données métropole de Brest (29)*, JO, n° 0213, 12 Sept. 2021, text n° 29.

55 Rennes Métropole, *Le service public métropolitain de la donnée 2017-2019 : deux années d'amorçage*, 2020, p. 32. Available at: https://rudi.fr/?BilanSpmd20172019DeuxAnneesDAmorcage (consulted on 19 June 2026).

56 Le Breton, M., Bailleul, H., Le Corf, J. and Mericskay, B., "La gouvernance des données urbaines entre territoire de projets et projet de territoire. L'exemple de Rennes Métropole", Flux , 2022, n° 127, p. 65-84.

57 Nantes métropole, Charte métropolitaine de la donnée, Site de Nantes métropole [online]. Available at: https://entreprises.nantesmetropole.fr/services-solutions/appliquer-la-charte-de-la-donnee-metropolitaine/ (consulted on 19 June 2026).

58 Brest métropole, Charte éthique de la donnée, Site de Brest métropole [online]. Available at: https://brest.fr/sites/default/files/medias/brestfr/documents/brest_ville_et_metropole/metropole/affichage_l%C3%A9gal/Charte_ethique_de_la_donnee.pdf (consulted on 19 June 2026).

59 Aix-Marseille-Provence, Charte métropolitaine de la donnée, Site de la métropole Aix-Marseille-Provence [online]. Available at: https://ampmetropole.fr/wp-content/uploads/2024/03/Charte-Metropolitaine-de-la-Donnee.pdf (consulted on 19 June 2026).

60 Rueil-Malmaison, Charte de la donnée, Site de la ville de Rueil-Malmaison [online]. Available at: https://www.villederueil.fr/sites/default/files/2019-11/a4_chartedonnee_2_web.pdf (consulted on 19 June 2026).

cisely, as to the effectiveness of their prescriptions. They are indeed classified among 'suggestive, indicative, incentivising and permissive means'[61], as distinct from the 'authoritative, binding, imperative and prescriptive means'[62] that ordinarily guide administrative action. The constraint charters place on private actors is accordingly rather weak. Nevertheless, the choice of the charter appears justified by its capacity to accommodate evolving practices and emerging risks in the field,[63] and thus by a deliberate reluctance to over-regulate a subject whose contours will become clearer at local level as the latest European regulations are implemented.

Licence-based governance offers another route to promoting the circulation of non-personal data. Already well established for public data, licensing also enables territorial authorities to bring private actors into a shared framework.[64] Licensing also enables territorial authorities to bring private actors into a shared framework. The *Métropole de Lyon* offers a notable example: in the field of mobility, it has created a *Licence de réutilisation des données d'intérêt général* [Licence for the Re-use of Data of General Interest], designed to open up public and private data on a sectoral basis while ensuring their use remains consistent with its public policies.[65]

2. *Institutional specialisation through dedicated structures*

Beyond a rationale grounded primarily in public service—though not without economic implications—the State, acting through public administration, also guarantees the circulation of non-personal data for commercial purposes. Territorial authorities have similarly established, or sought to establish, dedicated structures for the circulation of both public and private data.

One such initiative is the Occitanie Region's *Occitanie Data*. Launched in 2019 as an association, it aimed to 'propose a "trusted space" within the data economy, guaranteeing the rights of data owners'.[66] Its initial purpose was to create a framework conducive to data exchanges between public and private actors within the territory, so as to bolster the local economy. As the initiative proved successful, the association was converted in 2022 into a *Groupement d'intérêt public* [public-interest grouping] (GIP) under the name 'Ekitia', with a view to strengthening the data economy both within and beyond its territory. The new status will notably enable it to offer paid services to public and private data actors. Far from a merely cosmetic institutional choice—and echoing the *Métropole de Rennes*' decision to organise its own operations through a *régie*—the GIP Ekitia takes the form of

61 de Saint Sernin, J., "Les chartes administratives : Aporie du droit souple ?", *RDP* 2014, Librairie Générale de Droit et de Jurisprudence, nº 4, pp. 907-931.

62 Ibid.

63 Banque des territoires et Association internationale des Maires francophones, *Guide des chartes territoriales de la donnée*, 2023, p. 6.

64 Article L. 323-1 du *Code des relations entre le public et l'administration*.

65 See Courmont, A., "Chapitre 5. Les licences : instruments centraux du gouvernement par les données" in *Quand la donnée arrive en ville: Open data et gouvernance urbaine*, 2021, Presses universitaires de Grenoble, pp. 91-106; Aureau, T., Cytermann, L., Duchesne, C., Morel, M., Vachey., L., "Rapport relatif aux données d'intérêt général", *Rapport du Conseil Général de l'Économie, de l'Inspection Générale des Finances et du Conseil d'État*, 2015, p. 35.

66 Brouillet, S., "Economie de la donnée : l'association Occitanie Data planche sur des données « éthiques » et « souveraines »", *Gazette des communes*, 25 April 2019.

a *service public à caractère industriel et commercial* (SPIC), confirming a new role for territorial authorities within this economy.

Likely influenced by the preparatory work on the Data Governance Act, territorial data actors have turned to another structure capable of facilitating the sharing of non-personal data at local level: the data cooperative. In February 2020, the Rhône-Alpes regional platform *Apidae Tourisme*—originally established to 'pool resources for the development of a shared tourist information database'[67]—became a *Société coopérative d'intérêt collectif* [cooperative society of collective interest] (SCIC). The new status thus allows tourism actors, public and private alike, to pool their data and put them to productive use.

Though still uncommon in the French legal landscape, data cooperatives embody a mode of governance closely aligned with the spirit of the latest European regulations and, for that reason, are likely to gain further ground.[68]

Taken together, these initiatives seek to promote data circulation in ways that resemble what the Data Governance Act classifies as data-intermediation services, [69] though without sharing all of their characteristics.

These predominantly private services now occupy a central place in data circulation, both within and outside the administration. Yet the question arises as to the appropriate degree of public-sector involvement: is there merit in establishing public—or at least majority-public—structures to carry out such a mission?

The recent dissolution of *Agdatahub* affords an occasion for precisely this reflection. Dedicated specifically to agricultural data, the initiative aspired to become 'a portal for a competitive, open and sovereign French agriculture'.[70] Its aim was to improve data circulation for purposes reasonably referable to the general interest, such as monitoring pesticide use or decarbonising agriculture.[71] Unable to find a viable economic model, *Agdatahub*, like most private data-sharing infrastructures, called upon the State to step in, invoking the general-interest dimension of its activities.[72] Although the State had already

67 Bothorel, E., Combes, S., Vedel, R., "Pour une politique publique de la donnée", Report submitted to the Prime Minister on 23 Dec. 2020, p. 119.

68 See: Mannan, M., Wong, J., Bietti, E., "Data Cooperatives in Europe: A Preliminary Investigation", *Network Industries Quarterly* July 2022, Vol. 24, N°3, pp. 12–15; Bietti, E., Etxeberria, A., Mannan, M., Wong, J., "Data Cooperatives in Europe: A Legal and Empirical Investigation", White Paper created as part of The New School's Platform Cooperativism Consortium and Harvard University's Berkman Klein Center for Internet & Society, Research Sprint, Dec. 2021, [online]. Available at: https://cyber.harvard.edu/sites/default/files/2022-02/Data_Cooperatives_Europe-group2.pdf (consulted on 19 June 2026); Knapp, J., Kobler, J., Richter, P., "Data cooperatives–collective action as an opportunity for the european data economy and a european data private law", *Zeitschrift für Innovations-und Technikrecht (InTeR)* 2023, pp. 7–12.

69 For an exhaustive definition, see: recital n° 11 of article 2 - Definitions - of regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance), OJEU L 152 of 3 June 2022, pp. 1-44.

70 Picardat, S., "Apport de l'infrastructure de partage de données Agdatahub dans le secteur agri-agro", *Annales des Mines - Enjeux numériques, Quelles infrastructures numériques du futur ?*, 2024/3, n° 27, p. 137.

71 See Létourneau, L., "Plaidoyer pour les grandes oubliées : les infrastructures publiques de partage de données", *Annales des Mines - Enjeux numériques, Quelles infrastructures numériques du futur ?*, 2024/3, n° 27, p. 164; Létourneau, L., "Rapport sur les Infrastructures de données", *Terra Nova et Digital New Deal*, p. 48; Picardat, S., "Apport de l'infrastructure de partage de données Agdatahub dans le secteur agri-agro", *Annales des Mines - Enjeux numériques, Quelles infrastructures numériques du futur ?* 2024/3, n° 27, pp. 135 and 141.

72 Létourneau, L., "Rapport sur les Infrastructures de données", *Terra Nova et Digital New Deal*, p. 46.

intervened through the *Banque des Territoires* via several capital raises between 2020 and 2023, the transition to majority-public governance was not confirmed until the summer of 2024.[73] This proved insufficient to rescue the platform, which was placed in compulsory liquidation by judgment of 3 December 2024.[74] A private purchaser ultimately stepped in to take over the project[75], though not before a strategic infrastructure of the first order had passed out of public hands.

Whether the State should assume full or partial responsibility for such services remains an open question; what form and degree of intervention to adopt in this field is yet to be determined.

3. *Public administrations and the turn towards private data*

One last avenue—albeit a partial one—may open a new chapter in data circulation: the emergence in French law of 'data of general interest' or, more precisely, of what might be termed 'private data of general interest'. The *Administrateur général des données* [Chief Data Administrator] defines data of general interest as 'data relevant to the public, without any direct link to a public-service mission, whose release yields a general social benefit'.[76] The category originates from the recognition that certain data produced by private actors, outside any public-service mission, may prove highly valuable to public authorities and to citizens alike.

The notion of 'data of general interest' was first enshrined in the *loi pour une République numérique* [Law for a Digital Republic] of 2016,[77] which applied it to data relating to concession contracts, subsidy agreements, public statistics, judicial decisions, the public road domain, and property transfers. Beyond that statute, the same category appears in various sectoral regimes—transport, energy, health[78]—confirming that such data have acquired a distinct legal existence on a sector-by-sector basis.[79] Although the notion resists general definition, it lends itself to two complementary readings: a horizontal one, which promotes 'the use by administrations of data produced by the private sector';[80] and a vertical one, directed at 'data-sharing initiatives among private actors, for instance within a sector'.[81] The resulting constraint on private actors employing digital technologies across these fields is real, yet it operates within a general-interest rationale, obeying a public-service logic rather than a market logic.

The legal reach of this framework nonetheless appears questionable, insofar as it fails

73 Press release from the Ministry of Agriculture and Food Sovereignty, "Le conseil d'administration d'AgDataHub vote le passage de la société en gouvernance publique", 16 July 2024.

74 Announcement n° 2423 from BODACC A, n° 20240245, published on 19 Dec. 2024.

75 Decision of the *Tribunal des activités économiques* of Paris RG, n° 2025007682, 4 Feb. 2025.

76 Chief Data Administrator, "La donnée comme infrastructure essentielle", report to the Prime Minister on data in public administrations, La documentation Française, 2017, p. 19.

77 *Loi n°2016-1321 pour une République Numérique du 7 octobre 2016,* JO, 8 Oct. 2016, text n°1.

78 See on this specific point: Tifine, P., "Données privées d'intérêt général, Partage de données entre l'administration et le secteur privé", *JC. Adm.* 2024, Fasc. 109-90.

79 Ibid.

80 Bothorel, E., Combes, S., Vedel, R., "Pour une politique publique de la donnée", submitted to the Prime Minister on 23 Dec. 2020, p. 10.

81 Ibid.

to address contemporary challenges or meet the expectations of public actors, territorial authorities in particular. Data of general interest have fallen short of the ambitions that the grey literature projected onto them, yielding a legal category of modest scope whose very designation 'of general interest'—to borrow Professor Pierre Tifine's argument—may itself be open to doubt.[82] This difficulty may yet be resolved: EU law, French law, and the structures of State administration are all moving in that direction. EU law has now recognised the exchange of 'B2G' (Business to Government) data. The restrictive interpretation adopted at European level, however, consistent with the French approach, falls short of local actors' expectations. The obstacle that currently appears insurmountable concerns not whether such a mechanism should be free of charge or paid, but rather the question of consent: specifically, that of private economic operators to release their data. As matters stand, such data are either accessible on the basis of consent or, failing consent, within sectoral legal regimes, which in practice cover a relatively limited volume of data. The ultimate objective, nonetheless, remains to enable public administrations—the State and territorial authorities in particular—to access these data in the general interest, and above all in the service of their public-service missions.

B. Public economic law and the free circulation of data

While the plasticity of economic-regulation concepts suggests that digital data activities can be properly regulated, the challenges generated by the data economy reveal a need for conceptual renewal. In matters of data circulation, economic actors are caught between safeguarding an informational asset that constitutes a competitive advantage and sharing it: a course endowed, as it has been noted, with 'pro-competitive virtues'.[83] Competition thus makes room for a measure of cooperation and intermediation, so as to ensure the efficiency of the data economy,[84] a shift that is arguably paradigmatic. Such is the ambition underlying the Data Governance Act and the Data Act, both of which seek to secure this reconfigured model of data circulation.

The mechanisms examined above serve primarily the fulfilment of public service. They are not indifferent to the economic effects they produce, but their primary objective does not obey a commercial logic. Data circulation within the data market *stricto sensu* has not attracted comparable innovation or dedicated procedures; it rests, in the first instance, on a far more classical legal instrument: the contract[85] (1). Furthermore, the public administration, acting as economic regulator, oversees data circulation. To this end, it draws in part on specific legal innovations and, for the remainder, reinterprets the traditional concepts of economic-regulation law within the existing legal framework (2). Lastly, the economic regulation of data also follows a functional approach, whereby regulatory authorities cooperate so as to exploit the complementarity of their respective competences (3).

1. The contract as the principal vehicle for data circulation

82 Tifine, P. (2024), Données privées d'intérêt général, op. cit.

83 Brousseau, E., "Organiser la valorisation de l'or noir du XXIe siècle", *Annales des Mines - Enjeux numériques, Propriété et gouvernance du numérique,* 2022/2, n° 18, p. 16.

84 Ibid, p.16.

85 Conseil National du Numérique, *Avis sur la libre circulation des données dans l'Union européenne,* April 2017, p. 4.

'In practice, data circulation between distinct legal entities, or between legal and natural persons, rests largely on the technical handling of digital operations (controlling and restricting access, cryptography, and the like), together with contractual instruments, even where these are shaped by broader frameworks such as industrial and commercial secrecy or the protection of privacy. Ultimately, it is the contract that, above all, organises data circulation'.[86]

Such reasoning partly underlies the enactment of the Data Act, whose fifth recital states: 'Private law rules are key in the overall framework for data sharing. Therefore, this Regulation adapts rules of contract law and prevents the exploitation of contractual imbalances that hinder fair access to and use of data'.[87] In concrete terms, this takes the form of a Chapter IV devoted to 'unfair contractual terms related to data access and use between enterprises', composed of a single article entitled 'Unfair contractual terms unilaterally imposed on another enterprise', whose object is to forestall any contractual imbalance in the exploitation of data.

Public-law entities likewise resort to contracts in this area.[88] More precisely, contracts concluded by public bodies, and by local authorities in particular, address what becomes of any data engaged in their performance. Thus, although these are not commercial contracts for the sale or acquisition of data, 'data clauses'[89] are flourishing.

Local authorities are encouraged to make use of them, as with the 2024–2030 city contracts, which are to provide for 'the inclusion of clauses on the production of, provision of access to, and access to the data of the city contracts' co-signatories'.[90] It should however be specified that, as regards 'data of general interest' understood strictly within the meaning of the *loi pour une République numérique* [Law for a Digital Republic], and therefore within the framework of a public-service concession, these clauses appear rather as an expedient, arising where concessionaires fail to comply with their obligation to transmit such data to the granting authorities. Article 17 of the *loi pour une République numérique*, now codified at Articles L. 3131-2 and L. 3131-4 of the *Code de la commande publique* [Public Procurement Code], envisages an obligation to make the concessionaire's

86 Brousseau, E. (2022), Organiser la valorisation de l'or noir du XXIe siècle, op. cit., p. 20.

87 Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) (Text with EEA relevance), OJEU L 352 of 22 Dec. 2023, pp. 1-44.

88 For an exhaustive study on this subject, see: Cossalter, P., "Contrats publics et données", in Lanna, M. (dir.), *Smart city et prise de décision*, 2023, Mare & Martin, pp. 149–176.

89 See The 'Territorial Data Management Toolkit' developed by the Banque des territoires of the Caisse des dépôts: Banque des territoires, "Guide to Good Contractual Practices and Recommendations for Establishing a Territorial Data Governance Framework", 2021, Available at: https://www.banquedesterritoires.fr/sites/default/files/2021-01/20-211-BDT-Guide%20des%20bonnes%20pratiques%20contractuelles%20-%20web.pdf (consulted on 19 June 2026); Banque des territoires, "Data Management: What Tools and What Strategy for Territories?", 2021, Available at: https://www.banquedesterritoires.fr/sites/default/files/2021-01/20-103-BDT-Guide%20Gestion%20des%20donn%C3%A9es-web.pdf (consulted on 19 June 2026); Banque des territoires, *Note de lecture sur Cartographie des ensembles de données territoriales*, 2021, Available at: https://www.banquedesterritoires.fr/sites/default/files/2021-02/Note%20de%20lecture_carto_0.pdf (consulted on 19 June 2026).

90 *Circulaire du 31 août 2023 relative à l'élaboration des contrats de ville 2024-2030 dans les départements métropolitains.*

data available to the granting authority where they have been 'collected or produced in the framework of the operation of the public service that is the object of the contract and which are indispensable to its execution'. Insufficiently observed in practice, this obligation ought to be recognised for what it is: an extension of the *Conseil d'État*'s *Commune de Douai* judgment,[91] since the data must be returned to the granting public body, and at no cost.[92] Such data should not, therefore, be a bargaining chip between the contracting parties, but a '*bien de retour*' [return asset].[93]

Although the point does not concern France, which belongs to the legal order of the European Union and so falls within the territorial scope of the GDPR, a new use of contractual technique in the data field warrants a brief note. Contractual technique operates at the international level, through treaties, and more particularly through recourse to Digital Economy Agreements (DEAs) which, contrary to Preferential Trade Agreements (PTAs), no longer confine themselves to setting out traditional provisions on goods, services and intellectual-property rights, but organise a genuine regulatory framework for the digital economy.[94] Their new and more flexible approach allows States, in particular, to opt out of the full body of treaty provisions and thereby preserve room for a national strategy.[95]

The contract, then, whether private or public, probably constitutes the most 'reassuring' legal tool both for private economic operators and for the public administration. It provides a proven framework of trust, allowing private and public actors to define as precisely as possible the purposes for which their data circulate. The data economy is not, however, confined to contractual practice. For the rest, the law of economic regulation draws on its well-established concepts, subject, that is, to certain adaptations.

2. *Adapting the substantive law of economic regulation*

Over the past decade, the law of economic regulation has struggled to grasp the challenges posed by data. The difficulty lay partly in the complexity of applying the definition of a relevant market to digital platforms whose economic model rested essentially upon

91 See Boul., M., "Réflexions sur la notion de donnée publique", in Chevallier, J. and Cluzel-Métayer, L. (dir.), *Les données publiques, RFAP* 2018, n°167, p. 474; Cossalter, P., "Contrats publics et données", in Lanna, M. (dir.), *Smart city et prise de décision*, 2023, Mare & Martin, p. 159.

92 Dreyfus, J-D., "L'obligation du concessionnaire quant aux données et bases de données collectées ou produites à l'occasion de l'exploitation du service public", *AJCT* 2017, Dalloz, p. 185.

93 In the content of French law, the *biens de retour* are those used under a public service concession and that contribute directly to the fulfilment of the public service mission. Upon expiry of the concession agreement, these returnable assets must be handed over free of charge to the granting authority by the concessionaire previously responsible for the public service mission.

94 Burri, M., Vasquez Callo-Müller, M., Mesmert, A., "Digital Economy Agreements: A Path to Digital Trade Law 4.0?", *Trade, Law and Development*, 2025, Vol. XVII, n°1, p. 186-217.

95 See on Digital Economy Partnership Agreement (*DEPA*), the agreement between Chile, New Zealand and Singapore and South Korea: *"To enable flexibility and cover a wide range of issues, DEPA follows a modular approach that provides countries with more options to pick and choose and differs from the 'all- or-nothing' approach of conventional trade treaties"* in Burri, M., "Human Rights Implications of Digital Trade Law", *Trade, Law and Development*, 2025, Vol. XVI, n°2, p. 304.

the exploitation of data.[96] The way the relevant market was defined for the purposes of anticompetitive practices and merger transactions consequently had to evolve. The initial definition of 1997[97] was no longer suited to the digital economy, and so the European Commission updated it in 2024.[98]

This belongs to a broader effort to update the concepts of economic law and market regulation in response to the new demands of the platform economy, and of the data economy in particular. Two distinct regulatory approaches emerge: one, embodied by the *Autorité de la concurrence* [Competition Authority], favours adapting existing law within the current framework; the other, embodied by the European institutions, favours creating new concepts to meet these emerging challenges.[99]

From 2020 onwards, the *Autorité de la concurrence* opted for adapting the concepts of ex post economic regulation within the existing framework.[100] It recommended in particular, in matters of anticompetitive practices, the broadening of the notion of dominant position 'so as to include certain actors in a position of quasi-dominance, or on the point of tipping the market. This is the case with so-called *structuring platforms*[101] or, again, adapting the notion of essential infrastructure so as to extend it to 'certain databases, communities of users or ecosystems'.[102] It likewise supported the possibility of a renewed use of the procedural tools at its disposal, especially through provisional measures and binding undertakings. The *Autorité de la concurrence*, in matters of merger control, also recommended refining its competition analysis by incorporating factors specific to the digital sphere, such as potential competition from the major platforms; the extension of the analysis to non-tariff effects, such as pluralism or quality of service; extending the time horizon of the analysis, currently three to five years; and fuller account being taken of 'the collection, retention and exploitation of vast quantities of data'.[103] The *Autorité de la concurrence* therefore intends to take advantage of the adaptability of the existing tools to make use of them in a more proactive manner.

However, 'platforms, technically, economically and legally, escape in large part the national regulator'.[104] European Union intervention therefore proved necessary, to estab-

96 Arcelin, L., "Solidarisme et concurrence : une (ré)conciliation sur le terrain du marché numérique" in Castets-Renard, C. and Eynard, J. (dir.), *Un droit de l'intelligence artificielle : entre règles sectorielles et régime général*, 2023, Bruylant, p. 283.

97 Commission notice (97/C 372/03) on the definition of relevant market for the purposes of Community competition law of 9 Dec. 1997.

98 Commission notice (C/2024/1645) on the definition of relevant market for the purposes of Community competition law of 22 Feb. 2024.

99 Sée, A., "La régulation de l'économie numérique : l'émergence d'un droit des plateformes ?", in Bottini, F. (dir.), *Le droit (public économique) du monde d'après*, 2023, Legitech, pp. 60–61.

100 Autorité de la concurrence, "Contribution of the Competition Authority to the Debate on Competition Policy and Digital Challenges", 19 Feb. 2020. Available at: https://www.autoritedelaconcurrence.fr/sites/default/files/2020-02/2020.02.19_contribution_adlc_enjeux_numeriques_vf.pdf (consulted on 19 June 2026).

101 Ibid, p. 5.

102 Ibid.

103 Ibid, p. 11.

104 Bacache-Beauvallet, M., Bourreau, M., *IV / Régulation des plateformes. Économie des plateformes, La Découverte*, 2022, p. 83. Available at: shs.cairn.info/economie-des-plateformes--9782348075353-page-73?lang=fr (consulted on 19 June 2026).

lish *ex ante* regulation at European level complementing the *ex post* regulation provided by the *Autorité de la concurrence*.

This asymmetric *ex ante* regulation applies to gatekeepers, that is, those undertakings providing essential platform services in a position of lasting quasi-monopoly, with an annual turnover of at least 7.5 billion euros in the European Union over the last three years, or a market value of at least 75 billion euros, together with at least 45 million monthly end-users and at least 10,000 business users established in the EU.[105] The regulation is 'asymmetric' in that it 'imposes specific obligations on them and prohibits others'[106] and '*ex ante*' in that it 'does not merely adapt competition law and observe after the fact whether these gatekeepers comply with it'.[107] To date, the following are designated as gatekeepers: Alphabet,[108] Amazon,[109] Apple,[110] Booking,[111] ByteDance,[112] Meta[113] and Microsoft.[114]

This development in the law of economic regulation as applied to data is welcome, though not beyond reproach. As Professor Arnaud Sée notes,[115] the regulation carried out by the administration is 'problematically' fragmented. In France, this regulation is scattered between the CNIL [Data protection authority] for data and algorithms, ARCOM [Regulatory Authority for Audiovisual and Digital Communication] for content, the

105 Article 3 of Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance), OJEU L 265 du 12 October 2022, pp. 1-66.

106 Bacache-Beauvallet, M., Bourreau M., *IV / Régulation des plateformes. Économie des plateformes, La Découverte*, 2022, p. 88. Available at: shs.cairn.info/economie-des-plateformes--9782348075353-page-73?lang=fr (consulted on 19 June 2026).

107 Ibid.

108 Commission decision C(2023) 6101 final of 5th Sept. 2023 designating Alphabet as a gatekeeper pursuant to Article 3 of Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector.

109 Commission decision C(2023) 6104 final of 5th Sept. 2023 designating Amazon as a gatekeeper pursuant to Article 3 of Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector.

110 Commission decision C(2023) 6100 final of 5th Sept. 2023 designating Apple as a gatekeeper pursuant to Article 3 of Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector.

111 Commission decision C(2024) 3176 final of 13th May 2024 designating Booking Holdings Inc. as a gatekeeper pursuant to Article 3 of Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector.

112 Commission decision C(2023) 6102 final of 5th Sept. 2023 designating ByteDance as a gatekeeper pursuant to Article 3 of Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector.

113 Commission decision C(2023) 6105 final of 5th Sept. 2023 designating Meta as a gatekeeper pursuant to Article 3 of Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector.

114 Commission decision C(2023) 6106 final of 5th Sept. 2023 designating Microsoft as a gatekeeper pursuant to Article 3 of Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector.

115 Sée, A., "La régulation de l'économie numérique : l'émergence d'un droit des plateformes ?", op. cit., pp. 65–66.

ADLC [Competition authority] for competition aspects. Nevertheless, this co-regulation, problematic because of the fragmented handling of substantive law, is also an opportunity in functional terms, since it enables cooperation between the regulatory authorities, which bring their respective cutting-edge expertise to bear on a shared dialogue.

3. The functional approach: 'regulation throught data'

The functional approach is the use of data by regulatory authorities in carrying out their mission, as distinct from the substantive approach already considered, namely the law of economic regulation applied to data.

Regulatory authorities are bound up with the challenges that data present: they are able to gather the data that allow them to understand most fully the sector they oversee, in particular because 'it is, first of all, the possession of original, relevant, credible and complete information that enables them to carry out properly the missions entrusted to them'.[116] Although they may once have been disadvantaged by the information asymmetry between themselves and the regulated actors, the major digital platforms in particular, their growing command of data tends to redress the balance of power.[117]

In economic regulation, the early 2020s saw the competition authorities take a genuine interest in the data that enable them to carry out their mission.[118] The phenomenon is not new, however: the administrative courts have always been willing to grant regulatory authorities access to the data they need in order to perform their mission.[119] The real novelty, for these authorities, lies in building into their departments new specialist skills such as data mining[120] or data science.[121]

The gathering of information from regulated actors in the separate, compartmentalised manner described above no longer suffices on its own. The spread of digital technology and the growth of the data economy require the various fields of regulation to overlap. A further novelty, then, lies in a drawing-together of certain regulatory authorities, pooling their resources and sharing their expertise. Accordingly, in 2019 several regulatory authorities published a joint note on 'regulation through data'.[122] It sets out two main objectives: to strengthen the regulator's capacity to act, particularly in a supervisory role; and to inform users' choices and better steer the market.

The *Commission nationale de l'informatique et des libertés* (CNIL) and the *Autorité de la concurrence* (ADLC) have accordingly aligned their efforts in such a strategic way. Although the ADLC has been able, since 2007, to refer to any regulatory authority, including the

116 Mouchette, J., "Le recueil de l'information par les autorités de regulation", in Eckert G. and Kovar, J-P. (dir.), *La régulation économique et financière face aux défis de l'information*, 2018, L'Harmattan, p. 20.

117 Lombard, M., « La régulation par la donnée", *Le droit administratif au défi du numérique*, 2019, Dalloz, p. 169.

118 OECD - Directorate for Financial and Enterprise Affairs Competition Committee, *The future of leniency programmes: Advancing Detection and Deterrence of Cartels*, DAF/COMP/WP3(2023)1, 2023, p. 33.

119 Lombard, M., "La régulation par la donnée", op. cit., p. 158.

120 Ibid, p. 160.

121 OECD - Directorate for Financial and Enterprise Affairs Competition Committee, "The future of leniency programmes: Advancing Detection and Deterrence of Cartels", op. cit. p. 33.

122 New Regulatory Modalities – Regulation through Data, joint note of the Autorité de la concurrence, AMF, Arafer, Arcep, CNIL, CRE, CSA, 8 July 2019. Available at: https://www.arcep.fr/fileadmin/user_upload/grands_dossiers/La_regulation_par_la_data/note-aai-regulation-par-la-data-juil2019.pdf (consulted on 19 June 2026).

CNIL, for an opinion on matters within its field of competence,[123] the new cooperation strategy seems to raise this logic to another level, perhaps even in a major innovation, to the point of systematising it.

Thus, in December 2023, the two authorities signed a joint declaration entitled 'Competition and personal data: a common ambition', which set out their mutual expectations as follows: 'The economic exploitation of personal data thus brings together questions of competition and of data protection, and warrants particularly close cooperation between the two authorities in order to make the most of the existing regulatory synergies'.[124] For the ADLC, this means weighing the concerns of personal data protection in its decisions and, conversely, for the CNIL, weighing competition concerns in its own. In practice, the two authorities intend to go beyond the cooperation mechanisms provided by law and to work together more closely and informally, through regular exchanges and consultations, joint studies and staff training on shared concerns.[125] These commitments and their implementation were subsequently set out in greater detail by the CNIL's 2024 study on the interplay between data protection and competition.[126] This cooperation took concrete form in the 2025 decision by which the ADLC fined Apple 150 million euros for abuse of a dominant position[127] in connection with the American firm's rollout of its 'App Tracking Transparency' feature. In this case, the CNIL had issued two opinions[128] enabling the ADLC to be informed both on the technical specificities of the processes used by Apple and on their consequences in terms of personal data protection.

Taken together, the elements examined in this first part build up a distinctive conception, particular to the European Union, which stands out all the more sharply when a further variable, the protection of privacy, enters the data-circulation equation. It found its fullest expression in the ambitious GDPR which, having begun as a text promoting stronger protection for the data of European nationals, has since become the cornerstone of European data law. Yet, for all its established importance, mounting signs suggest that the European conception of privacy protection may be starting to give way before the demands of the market and intensifying competition in key sectors.

123 *Article R. 463-9 du Code de commerce.*

124 Autorité de la concurrence and Commission nationale de l'informatique et des libertés, "Concurrence et données personnelles : une ambition commune – Déclaration conjointe de l'Autorité de la concurrence et de la Commission nationale de l'informatique et des libertés", 12 Dec. 2023, p. 6. Available at: https://www.cnil.fr/sites/cnil/files/2023-12/concurrence_et_donnees_personnelles_une_ambition_commune_declaration_conjointe_cnil-adlc.pdf (consulted on 19 June 2026).

125 Ibid, p. 13.

126 Lasserre, B., *Conclusions de la mission de réflexion portant sur l'articulation entre protection des données et concurrence*, 28 Nov. 2024, pp. 32 – 39. Available at: https://www.cnil.fr/sites/cnil/files/2024-12/rapport_mission_lasserre.pdf (consulted on 19 June 2026).

127 Autorité de la concurrence, *Décision n°25-D-02 du 31 mars 2025 relative à des pratiques mises en œuvre dans le secteur de la publicité sur applications mobiles sur les terminaux iOS.*

128 CNIL, Deliberation No. 2020-137 of 17 Dec. 2020 issuing an opinion in the context of the complaint filed by certain professional associations of online advertising against Apple Inc. before the Competition Authority (request for opinion No. 20019591); CNIL, Deliberation No. 2022-060 of 19 May 2022 issuing an opinion in the context of the complaint filed by certain professional associations of online advertising and online service publishing against Apple Inc. before the Competition Authority (request for opinion No. 22009231).

II. Personal data and public administration: a compromise between circulation and protection

Personal data receive particular attention in the European Union, to the point that it has built a genuine model around this concept (A). The demands of competitiveness, driven above all by AI, may nonetheless call that model into question (B).

A. Adapting the principle of free data circulation to ensure protection

Data protection may at times elicit a degree of mistrust among private economic actors, who see in it a symbol of bureaucracy, associated above all with the compliance procedures imposed by the GDPR. Yet, far from holding economic development back, the protection of personal data may even drive it forward (1).

Nor does this duty of GDPR compliance fall on private operators alone: the public administration is equally bound by it (2). Lastly, although it inevitably entails additional administrative effort, the protection of personal data stands as a priority in a globalised economy, all the more so where that economy is dominated by actors from outside the European Union (3).

1. The myth of personal data protection as hostile to economic development

'*Personal data, namely those relating to an identified or identifiable natural person, now represent a major economic asset for undertakings, which increasingly build their strategies on the exploitation of such data*'.[129] One might therefore suppose that the chief limit on data circulation lies in the protection of personal data. That assumption is quickly dispelled.

Although the regulation of 14 November 2018 establishes a framework applicable to the free circulation of non-personal data,[130] it does not overlook the need to dovetail with the GDPR, providing for 'a coherent set of rules concerning the free circulation of different types of data'.[131]

The GDPR likewise lays down this principle of free circulation for personal data. As Article 1(3) specifies: 'the free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data'. Both the regulation on non-personal data flows and the GDPR thus adopt markedly liberal principles.

Thus, although one might have feared that the goal of personal-data protection would hold back the development of digital technology, ruling out any release of data by administrations or any reuse by third parties, nothing of the kind has come to pass. Individuals must indeed be protected against the risk of intrusion into their privacy, and both French law and European Union law work to that end; yet the turn to digital technology and the circulation of data serve not only to develop the economy but also to modernise public services and improve those offered to users. The *Autorité de la concurrence* has, moreover, already observed that the protection of personal data contributes to the com-

129 Lecourt, A., "Droit de la concurrence et numérique", *Répertoire IP/IT et Communication* 2019, Dalloz.

130 Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 Nov. 2018 on a framework for the free flow of non-personal data in the European Union (Text with EEA relevance), OJEU L 303 du 28 Nov. 2018, pp. 59-68.

131 Ibid, Recital n° 10.

petitive dynamics of markets.[132]

The economic impact of data protection has often been criticised in the economic literature,[133] which has repeatedly sought to link compliance with the GDPR to significant costs, and even to falls in profits for undertakings.[134] Yet, in the wake of the colloquium '*GDPR: what economic impact?*'[135] organised by the CNIL in collaboration with the *Direction générale du Trésor* [Directorate General of the Treasury], the conclusions drawn from the contributions of the specialists revealed how relative the cost of GDPR compliance in fact is. It might, on the contrary, generate positive externalities, in that GDPR compliance would prompt a 'rationalisation of data processing and better use of the data held by undertakings'.[136]

The reality is no doubt more nuanced. While both advantages and drawbacks are probably observable, the better question is how they affect the actors concerned. On this point, the CNIL itself admits that 'the GDPR is proportionally more favourable to large economic actors, which have more means to devote to compliance'.[137] Conversely, for smaller actors, compliance with data protection is 'a complex, time-consuming and costly task in the face of which data controllers stand unequal, given the financial and human resources at their disposal'.[138] Although no negative economic impact is established, an imbalance nonetheless persists, favouring the 'large' at the expense of the 'small'. The CNIL, for its part, takes a clear-eyed view of its role: on the one hand, it must 'actively offset this tendency through a demanding policy towards the large actors, and all the more towards the very large, in proportion to the risks they pose and the means at their dis-

132 Autorité de la concurrence, *Décision n°22-D-12 du 16 juin 2022 relative à des pratiques mises en œuvre dans le secteur de la publicité sur internet*, § 247.

133 The CNIL considers these studies to be incomplete and reproaches them for an unsuited experimental approach. See in this sense: "L'impact économique du RGPD, 5 ans après", website of CNIL, 1 March 2024. Available at: https://www.cnil.fr/fr/limpact-economique-du-rgpd-5-ans-apres (consulted on 19 June 2026).

134 Chen, C., Benedikt Frey, C., Presidente, G., "Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally (Working paper)", *The Oxford Martin Working Paper Series on Technological and Economic Change*, 2022. Available at: https://oms-www.files.svdcdn.com/production/downloads/Privacy-Regulation-and-Firm-Performance-Giorgio-WP-Upload-2022-1.pdf; Jia, J., Jin, G.-Z., Wagman, L., *The Short-Run Effects of GDPR on Technology Venture Investment*, 2019. Available at: https://ssrn.com/abstract=3278912; Goldberg, S., Johnson, G., Shriver, S., "Regulating Privacy Online: An Economic Evaluation of the GDPR", *American Economic Journal: Economic Policy*, 2019. Available at: https://ssrn.com/abstract=3421731.

135 Colloquium "RGPD : quel impact économique ?" of 20 May 2025 organised by the CNIL and the Direction générale du Trésor. Replay available at: https://www.cnil.fr/fr/participez-levenement-rgpd-quel-impact-economique-le-20-mai-2025 (consulted on 19 June 2026).

136 According to Sam Ruiqing Cao, Assistant Professor at Stockholm school of economics at the event "RGPD : quel impact économique ?" Organized by the CNIL and the Direction générale du Trésor the 20 May 2025. Available at: https://www.cnil.fr/fr/evenement-rgpd-quel-impact-economique-compte-rendu-des-debats. Reply available at: https://www.cnil.fr/fr/participez-levenement-rgpd-quel-impact-economique-le-20-mai-2025 (consulted on 19 June 2026).

137 CNIL, "L'impact économique du RGPD, 5 ans après", 1 March 2024. Available at: https://www.cnil.fr/fr/limpact-economique-du-rgpd-5-ans-apres (consulted on 19 June 2026).

138 Pailler, L., "Chapitre 2 – Le droit de la protection des données à caractère personnel", *Précis Droit des activités numériques*, 2023, Dalloz, reference point n° 103.

posal'[139] and, on the other hand, to support the smaller actors which have need of it.[140]

Finally, seeking to assess the economic impact of its policies more accurately, the CNIL, in its work programme for 2026–2028,[141] announced the creation of an economic-analysis unit with two objectives: 'to deepen the understanding of business models linked to personal data and to better measure the economic impact of CNIL decisions'. It thereby intends to develop its study of business models founded on personal data and to refine its standing on economic regulation.

2. The legal regime governing inter-administration data exchanges, as shaped by personal data protection

The modernisation of the public administration has made simplification of the relationship with the public a priority. The aim is now to spare the public, wherever possible, the administrative burden of procedures that are sometimes onerous and often redundant. Such simplification rests in large part on reducing the demands made on the public to supply information. For undertakings, the cost of the administrative burden is estimated at three to five per cent of GDP,[142] a figure that has prompted the public administration to give practical effect to modernisation and simplification through the digitisation embodied in the 'tell us once' programme,[143] which now constitutes a genuine principle of administrative action.[144] The scheme is estimated to save undertakings 200 million euros a year in management costs.[145] Initially tested and refined in public-procurement procedures,[146] it has since been extended, more broadly, to dealings between individuals and the public administration. The resulting dynamic would go on to shape the legal regime of inter-administration data exchange profoundly, a regime built up in two stages.

139 CNIL, "L'impact économique du RGPD, 5 ans après", op. cit.

140 See: CNIL, "Accompagnement des professionnels : le programme de travail de la CNIL pour 2025", 27 March 2025. Available at: https://www.cnil.fr/fr/accompagnement-des-professionnels-le-programme-de-travail-de-la-cnil-pour-2025 (consulted on 19 June 2026); CNIL, "Accompagnement des professionnels : le programme de travail de la CNIL pour 2026", 7 April 2026. Available at: https://www.cnil.fr/fr/accompagnement-des-professionnels-le-programme-de-travail-de-la-cnil-pour-2026 (consulted on 19 June 2026).

141 CNIL, "Économie de la donnée : la CNIL publie son programme de travail pour 2026-2028", 2 February 2026. Available at: https://www.cnil.fr/fr/economie-de-la-donnee-la-cnil-publie-son-programme-de-travail-pour-2026-2028 (consulted on 19 June 2026).

142 Sorin, C., "Dites-le nous une fois : un programme qui simplifie la vie des entreprises", *Documentaliste-Sciences de l'Information*, vol. 51, n° 4, 2014, pp. 36–38.

143 *Arrêté du 1er juillet 2013 modifiant l'arrêté du 30 octobre 2012 portant organisation du secrétariat général pour la modernisation de l'action publique.*

144 Didriche, O., "Chapitre 4 – Marchés publics : sélection des candidatures et des offres", *Encyclopédie des collectivités locales*, 2023, Dalloz, reference point n° 65 –"Accès des acheteurs"; Cassar, B., "Section 2 - Les modalités d'accès aux données", *Répertoire IP/IT et Communication*, Données – Gouvernance des données IP/IT, 2022, Dalloz, reference point n° 35 "Partage des données et mise en commun"; *Décret n° 2016-1971 du 28 décembre 2016 précisant les caractéristiques du formulaire unique de demande de subvention des associations*, JO n°0303 of 30 Dec. 2016, text n° 149.

145 Delaunay, B. et al., "Chronique de l'administration", *Revue française d'administration publique (RFAP)* 2015/3 N° 155, p. 804.

146 *Décret n° 2014-1097 du 26 septembre 2014 portant mesures de simplification applicables aux marchés publics, texte n° 31.*

At the first stage, the legal regime of inter-administration data exchange was set within a general framework addressing both the demands of a simpler relationship with the public and the public administration's growing use of digital technology. It was instituted and generalised in 2011 by the *loi de simplification et d'amélioration de la qualité du droit* [law on the simplification and improvement of the quality of the law].[147] Considerations of personal data protection enter into this regime from the outset. First, a principle of strict necessity governs these exchanges: only the data strictly necessary to process the user's request may be exchanged. A correlative obligation to inform complements this principle: the public administration must tell users which data are needed to process their request and identify those it will obtain from other administrative authorities. Lastly, a right of access to and rectification of data is afforded to the user. These provisions were subsequently codified in the *Code des relations entre le public et l'administration* [Code of Relations between the Public and the Administration],[148] before being supplemented by the *loi pour une République numérique* [Law for a Digital Republic] of 2016.[149] The latter clarified that business secrecy is not opposable to inter-administration data exchanges: where the law empoers an administration to obtain such data in the exercise of its functions, no claim of commercial confidentiality may stand in the way. Lastly, the *loi pour un État au service d'une société de confiance* [Law for a State Serving a Society of Trust] of 2018 (the 'ESSOC' law),[150] reinforced the 'tell us once' principle by granting undertakings the right not to 'provide an administration with information it already holds in an automated processing system, or that can be obtained from another administration through such a system'.[151]

At the second stage, the legal regime of inter-administration data exchange had to be reconciled with the concerns of personal data protection as renewed by the GDPR. By way of experiment, two decrees were adopted in 2019 to bring this regime into line with the protection of personal data. One of the first measures replaces the requirement to obtain consent with a requirement to inform the user of the use that will be made of their data.[152] This was a bold choice, marking the government's determination to harmonise relations between the administration and the public, but also and above all to extend ad-

147 Article 4 of the *loi n° 2011-525 du 17 mai 2011 de simplification et d'amélioration de la qualité du droit* (Law on the Simplification and Improvement of the Quality of Law) introduced new provisions by creating Article 16A of the *loi n° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations* (Law on the Rights of Citizens in their Relations with Public Authorities). This article laid the foundations for the legal framework governing data exchanges between public authorities, addressing the challenges posed by the digitalisation of such exchanges while integrating safeguards for the protection of users' privacy.

148 *Ordonnance n° 2015-1341 du 23 octobre 2015 relative aux dispositions législatives du code des relations entre le public et l'administration.*

149 *Article L114-8 du Code des relations entre le public et l'administration tel que modifié par l'article 91 de la loi n°2016-1321 du 7 octobre 2016 pour une République numérique.*

150 *Loi n° 2018-727 du 10 août 2018 pour un État au service d'une société de confiance du 10 août 2018,* JORF n°0184 of 11 Aug. 2018, text n° 1.

151 *Article 40 de la loi n° 2018-727 du 10 août 2018 pour un État au service d'une société de confiance,* JO of 11 Aug. 2018, text n° 184.

152 *Article 6 du décret n° 2019-31 du 18 janvier 2019 relatif aux échanges d'informations et de données entre administrations dans le cadre des démarches administratives et à l'expérimentation prévue par l'article 40 de la loi n° 2018-727 du 10 août 2018 pour un Etat au service d'une société de confiance,* JO of 20 Jan. 2019, text n° 68.

ministrative simplification through digitisation.

The most significant advances in this matter were brought about by Article 162 of the so-called '3DS' law.[153] First, it extends to all users the right not to supply an administration with information that the administration already holds or could obtain from another administration. To keep the 'tell us once' scheme working properly and durably, the '3DS' law gives priority to informing the user over obtaining their consent. It also, however, affirms a right to object to the continued processing of data, for the benefit of the user.

The advance deserves qualification, however, since the user may express a refusal only upon each initial request for a data exchange. In other words, the law establishes an opt-out mechanism within the 'tell us once' scheme, placing the individual back at the centre of the legal regime governing inter-administration data exchanges. Alongside this right to object, the user enjoys rights of access to, and rectification of, the personal data subject to such exchanges. Although the GDPR-compliance dimension of the legislation is notable, it remains limited: the law prioritises informing the user over obtaining consent, and the right to object extends only to the first request formulated by the administration. The tempering of the GDPR philosophy within this regime reflects the broader ambition it serves—a better administration: digital, simple, and accessible to all. The final and arguably most significant contribution of Article 162 of the *loi relative à la différenciation, la décentralisation, la déconcentration et portant diverses mesures de simplification de l'action publique locale* [Law on Differentiation, Decentralisation, Deconcentration and Various Measures for the Simplification of Local Public Action] (the afore-mentioned '3DS' law) lies in the exchange of data aimed at informing users of their entitlement to a benefit or advantage, extending to the point of securing it on their behalf. The innovation is a major one, reversing the traditional direction of the relationship between administration and administered in the context of applications for benefits. The process is no longer ascending, whereby the user applies to the administration to obtain a right, but descending: one that goes beyond merely informing the user of a right's existence and proceeds to execute it for them.

3. Personal data protection as a matter of sovereignty

At first sight, a limit on data circulation—including, crucially, non-personal data—might be tied not to a civil-liberties concern but to one of sovereignty, bound up with considerations of public security.

Free data circulation implies, in particular, that public-law entities may store data beyond the borders of the State to which they belong. This follows from recital 13 of the 2018 Regulation on the free flow of non-personal data[154] which promotes 'greater freedom of choice as regards suppliers of data-focused services, more competitive prices'. Data originating from the State's administrative bodies, or from other public-law entities, may therefore be stored beyond the borders of their national territory, which can give rise to

153 *Article 162 de la loi n° 2022-217 du 21 février 2022 relative à la différenciation, la décentralisation, la déconcentration et portant diverses mesures de simplification de l'action publique locale*, JO of 22 Feb. 2022, text n° 3.

154 Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Text with EEA relevance), OJEU L 303 of 28 November 2018, p. 59-68.

difficulties, as the storage of COVID-19 health data on Microsoft tools made plain.[155]

A restriction on free circulation is, however, provided for on grounds of public security, for which the Member States must account to the European Commission, as Article 4 of the Regulation on the free flow of non-personal data provides. As recital 19 of the same text specifies, the concept covers 'the internal or external security of a Member State', the 'detection of criminal offences', and prosecutions and investigations. It also presupposes a 'genuine and sufficiently serious threat affecting one of the fundamental interests of society', such as the functioning of institutions or essential public services, or 'for the survival of the population', the 'risk of a serious disruption to external relations or to the peaceful coexistence of nations', or a 'risk to military interests'.

The sovereignty-based approach is well attested in the case law of the Member States, where the concern bears less on the circulation of certain personal data than on their retention, as the *Conseil d'État, Assemblée judgment of 21 April 2021, French Data Network et autres, illustrates*.[156] The ruling followed a decision of the Court of Justice holding that French law, in permitting the 'general and indiscriminate retention' of data for criminal and intelligence purposes, is manifestly incompatible with European Union law.[157] Unlike the German Federal Constitutional Court in its decision of 5 May 2020 on the powers of the European Central Bank, the *Conseil d'État*, notwithstanding the French government's express request, declined to carry out an '*ultra vires* ' review,[158] that is, a review of whether the EU authorities had kept within their field of competence. It nonetheless accorded constitutional rules precedence over certain provisions of the contested legislation, relying on the principle that

> *'in the case where the application of a European directive or regulation, as interpreted by the CJEU, would have the effect of depriving one of [the] constitutional requirements, which*

155 See Tifine, P., "Health Data hub doit prendre des garanties supplémentaires en vue de limiter le risque de transfert de données personnelles de santé vers les États-Unis : Chronique de droit de l'administration numérique - juin/novembre 2020", *Lexbase Public*, January 2021.

156 Conseil d'État, 21 April 2021, n°393099, *French Data Network et autres*. See: Rec., p. 62, concl. Lallet; Malverti C., Beaufils, C., "L'instinct de conservation", *AJDA* 2021, Dalloz, p. 1194; Belkacem, N., "Données de connexion - La conciliation par le Conseil d'État du respect du droit de l'Union européenne et de l'efficacité de la lutte contre le terrorisme et la criminalité : les données de connexion", *Communication - Commerce électronique*, n°7-8, 2021, Lexis Nexis, reference point n°56; Simon, D., "Retour des monologues juridictionnels croisés ? – À propos de l'arrêt du Conseil d'État dans l'affaire « French Data»", *Europe*, 2021, n°6, Lexis Nexis, reference point n°3; Bartolucci, M., "Le Conseil d'État acte la conservation générale et indifférenciée des données de connexion", *La Semaine Juridique - Administrations et collectivités territoriales (JCP A)*, 2021, n°28, Lexis Nexis, reference point n°2223; Iliopoulou-Penot, A., "La conservation généralisée des données de connexion validée, le droit au désaccord avec la Cour de justice revendiqué", *La Semaine Juridique - édition Générale (JCP G)*, 2021, n°24, Lexis Nexis, reference point n° 659; Lallet, A., "Données personnelles : droit de l'Union européenne et Constitution – Conclusions sur Conseil d'État, assemblée, 21 avril 2021, French Data Network et autres , n° 393099 et autres", *Revue française de droit administratif*, n°03, Dalloz, p. 421.

157 CJUE, 6 Oct. 2020, case n° C-511/18, *La Quadrature du Net and others*, case n° C-512/18, *French Data Network and others*, and case n° C-520/18, *Ordre des barreaux francophone et germanophone and others*; See also CJUE, 6 Oct. 2020, case n° 623/17, *Privacy International c/ Secretary of State for Foreign and Commonwealth Affairs and others*; See finally CJUE, 2 March 2021, case n° C-746/18, *H. K. c/ Prokuratuur*.

158 BVerfG., 5 May 2020, *PSPP (Public Sector Purchase Programme)*, 2 BvR 859/15.

would not benefit, in Union law, from equivalent protection, of effective guarantees, the administrative judge, seised of a plea to that effect, must set it aside in the strict measure that respect for the Constitution requires'.[159]

B. The European model between free circulation and data protection

In every capacity in which it operates on the market, the public administration may soon confront a fundamental reshaping of personal data protection law. The law governing data circulation extends well beyond French administrative law and is largely shaped by EU law. By projecting itself beyond Europe's borders, the European model is at once exported and imposed (1). Its founding conception, built essentially around data protection, may nonetheless give way to the competitive imperatives unleashed by the race for AI (2).

1. Asserting the European model through the extraterritorial reach of personal data protection law

Free data circulation, in the digital data economy generally and in that of artificial intelligence in particular, also presupposes the movement of data across space. What is termed 'transborder data flows', or 'cross-border data flows', is nothing new. As early as 1980, the interministerial report on 'transborder flows of information and data' noted the need for cooperation among European States in order to 'establish common standards of data protection, capable of guaranteeing individual freedoms while preserving the free circulation of information'.[160] The 'primary concern' already lay with the unlawful use of the data, or rather information, transferred abroad; it was also recognised that, given the state of the art at the time, transferring data abroad effectively removed them from the law of their country of origin.[161] Two courses were therefore open: 'either to organise, within international law, a harmonisation of the principles of protection, the path followed by both the Council of Europe and the OECD; or to organise, through bilateral agreements or conventions, a 'right of pursuit' by national legislation over data leaving for abroad, a path that has so far scarcely been explored'.[162]

This assessment, now outdated following the birth of the European Union, the creation of a dedicated body of law and the adoption of the GDPR, already carried the seeds of one of its key features: extraterritoriality. By allowing the GDPR to operate beyond the borders of the European Union, extraterritoriality strengthens the personal data protection of European nationals against the legislation of non-member States.[163] The influence of this extraterritoriality on foreign laws is far from negligible, in substance as well as on

159 Conseil d'État, 21 April 2021, n°393099, *French Data Network et autres*, recital n° 5.

160 Madec, A., *Les flux transfrontières d'informations et de données, dans « Les flux transfrontières de données : vers une économie internationale de l'information »*, 1982, La Documentation française, p. 12.

161 *Loi n° 68-678 du 26 juillet 1968 relative à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères*, JO of 27 July 1968, p. 7267.

162 Madec, A., "Les flux transfrontières d'informations et de données", op. cit., p. 14.

163 Castets-Renard, C., *Droit du marché unique numérique et intelligence artificielle*, 2020, p. 27.

the institutional landscape. The latest alignment of United States law with European law through the Data Privacy Framework, for instance, led to the creation of the Civil Liberties Protection Officer within the Office of the Director of National Intelligence, whose decisions may be appealed to the Data Protection Review Court.[164]

In data protection, the requirement that data flows outside the EU meet an adequate level of protection is telling of the Union's ambition to have its sovereignty respected in the digital space, both by other States and by the major platforms.[165]

This sovereignty over personal data protection, though plainly built strategically through European regulation, has equally been built through the case law of the Court of Justice, in response to incursions on its law beyond its borders. It first established a 'digital sovereignty through the norm' by regulating digital activities directly[166] and by guaranteeing the protection of the personal data of European nationals. The Cloud Act, for instance, which grants a right to disclose the data of European nationals at the discretion of American private operators, thus illustrated a form of 'interference'[167] and entered directly into conflict with the provisions of the GDPR. This sovereignty then took hold through the case law of the European Court of Justice, which 'boldly and forcefully raised the protection of personal data to the status of an essential principle of an emerging European digital sovereignty'.[168] The *Schrems 1*[169] and *Schrems 2*[170] exemplify the trajectory by which the CJEU invalidated the decisions of the European Commission acknowledging the adequacy of the personal data protection guaranteed by the Safe Harbour (*Schrems 1*) and then by the Privacy Shield (*Schrems 2*). These mechanisms qualified the so-called 'through the norm' sovereignty[171] guaranteed by the GDPR, and in ruling as it did the Court of Justice reaffirmed its proactive conception of a European digital sovereignty.

The sovereignty over personal data protection is also the product of the European Union's regulatory strategy, which has sought to impose constraints on a digital ecosystem initially left unregulated to foster its growth.[172] The shift is arguably paradigmatic: an ordoliberal European response, attentive to fundamental rights, and to privacy in particular, to the growth of digital technology within the neoliberal framework that prevailed from the 1990s onwards.

164 Commission Implementing Decision (EU) 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework (notified under document C(2023)4745), JOEU, L 231, 20 Sept. 2023.

165 Castets-Renard, C., "Souveraineté étatique et plateformes numériques : vers une coopération au sein du DSA ?", in Bertrand, B. and et Le Floch, G. (dir.), *La souveraineté numérique*, 2024, p. 51.

166 Terpan, F., "La conception européenne des enjeux de souveraineté numérique", in Bertrand, B. and Le Floch, G. (dir.), *La souveraineté numérique*, 2024, p. 184.

167 Bénabou, L., "La Cour de justice, gardienne d'une 'souveraineté européenne' sur les données personnelles", *RAE*, 12 Oct. 2018, p. 27.

168 Ibid, p. 19.

169 CJEU, 6 Oct. 2015, case n° C-362/14, *Maximillian Schrems c/ Data Protection Commissioner.*

170 CJEU, 16 July 2020, case n° C-311/18, *Data Protection Commissioner c/ Facebook Ireland Limited, Maximillian Schrems.*

171 Terpan, F., "La conception européenne des enjeux de souveraineté numérique", *in* Bertrand, B. and Le Floch, G., (dir.), *La souveraineté numérique*, 2024, p. 186.

172 Frydman, B., "Chapitre II. Comment penser le droit global ?", in *La science du droit dans la globalisation*, 2012, Bruylant, pp. 17-48.

Such an opposition belongs, in truth, to a broader phenomenon: that of *lawfare*, the strategic use of law. The contest over the control or protection of data through the extraterritoriality of norms is not recent. As early as 2001, in the wake of the 11 September attacks, the United States equipped itself with an intrusive legal instrument concerning data held abroad, in section 215 of the Patriot Act. Edward Snowden's revelations in 2013 led to the repeal of section 215, ostensibly ending this collection of telephone data. In 2018, however, the United States adopted the Cloud Act, allowing the American authorities, in the course of their investigations, to access the data of users of American communication and cloud services, even where those data are hosted on servers abroad: 'Whereas the place of storage of data was hitherto the criterion for determining the applicable legislation'.[173] More recently still, on 20 April 2024, by adopting the Reforming Intelligence and Securing America Act (RISAA), the American Congress extended for a further two years section 702 of the Foreign Intelligence Surveillance Act (FISA), which allows the federal intelligence services to collect data on individuals outside the territory.[174] As regards its scope of application: 'section 702 of the Foreign Intelligence Surveillance Act (FISA) permits [...] the American intelligence services to proceed with a targeted surveillance of foreign persons situated outside the United States by constraining the American suppliers of electronic communication services to communicate data to them'.[175] It should be noted that, where lawfare is applied to the control or protection of data, the concerns are not solely transatlantic. The Chinese National Intelligence Law of 28 June 2017, which allows the Chinese intelligence agencies to collect data in bulk,[176] likewise warrants vigilance.[177]

At a time of constant rivalry between States in the race for artificial intelligence, there can be no doubt that European digital sovereignty in personal data protection will find new forms of expression in the case law of the CJEU. The European Commission has itself restated the firmness of its position on the global application of the law protecting European nationals' personal data in the field of artificial intelligence: 'the Commission is convinced that international cooperation on AI matters must follow an approach that promotes respect for fundamental rights, in particular human dignity, pluralism, inclusion, non-discrimination and the protection of privacy and personal data, and it will strive to export the EU's values throughout the world'.[178]

This trend, readily apparent in European regulation and case law, is not confined to verifying the adequacy of data protection in States outside the Union. It is meant to extend wherever the protection of personal data is at stake. Given Europe's weight in the

173 Pierucci, F. and Guillerme, P., "Extraterritorialité du droit en matière de compliance : vers la fin de la sécurité juridique pour les entreprises européennes ?", *Revue de l'Union Européenne*, 2023, p. 603.

174 El Hilali, K., "La section 702 de la loi FISA : un outil de surveillance domestique contraire à la Constitution ?", *Revue du droit public*, Dec. 2024, p. 98.

175 G'sell, F., "L'avenir incertain des flux de données transatlantiques", *Annales des Mines - Enjeux numériques - La souveraineté numérique : dix ans de débats, et après ?*, 2023/3 N° 23, p. 26.

176 d'Agrain, H., "Europe : la souveraineté numérique au défi de l'autonomie technologique", *Annales des Mines - Enjeux numériques - La souveraineté numérique : dix ans de débats, et après ?*, 2023/3, n° 23, p. 64.

177 Houlié, S., *Rapport public fait au nom de la délégation parlementaire au renseignement relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2022-2023*, p. 42.

178 European Commission, "White paper on On Artificial Intelligence - A European approach to excellence and trust", Bruxelles, 19 Feb. 2020, COM(2020) 65 final, p. 10.

market, the disputes that arise over the compliance of AI models with the GDPR will, at the very least, encourage adherence to stricter rules, and may even set a standard in the field.

By way of example, the *Garante per la protezione dei dati personali*, the Italian personal data protection authority, fined OpenAI 15 million euros following the launch of ChatGPT, by a decision of 2 November 2024[179] for breaches of the GDPR concerning the protection of personal data. The penalty is coupled with an obligation to run a six-month public-information campaign on how ChatGPT works, addressing in particular the 'right of data subjects to object and to have their personal data erased', together with a notification to the Irish data protection authority, the lead authority under the one-stop-shop procedure.[180] The Italian data protection authority faults OpenAI, in particular, for failing to notify it of a data breach it suffered in March 2023; for using personal data to train ChatGPT without any appropriate legal basis; for breaching the principle of transparency and the related information obligations towards users; and, finally, for failing to provide age-verification mechanisms, thereby potentially exposing children under 13 to inappropriate responses.

This decision was published at the same time as an opinion of the European Data Protection Board (EDPB) on data protection in the training of the various AI models.[181] The opinion allows for an informed assessment both of the Italian authority's recent decision and of the GDPR's impact on data circulation in the age of artificial intelligence. It reaffirms the fundamental principles protecting individuals, notably the anonymisation of data, on which the EDPB notes that AI models cannot be regarded as anonymous by nature and must be assessed case by case.[182] It then notes that 'there is no hierarchy among the legal bases provided for by the GDPR and that it is for the data controllers to identify the appropriate legal basis for their processing activities', thereby not ruling out, in effect, dispensing with the consent of the persons whose data are processed in favour of the legitimate interest of the body processing them. In such a case, however, it points to the requirement of the 'three-part test': identifying the legitimate interest, assessing necessity, and confirming that the interests or fundamental rights and freedoms of the persons concerned do not override it.[183] Finally, it sets out the various scenarios in which the unlawful processing of data during the development of an AI model may affect the subsequent processing or use of that model.[184] The EDPB thereby offers an analysis of particular insight and importance for the future of personal data protection in the AI context, acknowledging that 'the unlawfulness of the processing during the development phase may have a bearing on the lawfulness of the subsequent processing'. In other words, the unlawfulness affecting an AI model would, in certain cases, set off a chain reaction, rendering unlawful in turn the other processing operations that rely on it. The supplier's failing thus becomes the clients' failing where data processing is non-compliant from the

179 *Garante per la protezione dei dati personali, Provvedimento del 2 novembre 2024*, n°10085455 (Italian Data Protection Authority (Garante), Decision of 2 Nov. 2024).

180 See article 4.23 of GDPR on "cross-border processing".

181 European data protection board, opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models, adopted on 17 Dec. 2024.

182 Ibid, p. 14.

183 Ibid, p. 2.

184 Ibid, pp. 31-35.

design of the model onwards. On this view, it seems scarcely conceivable that undertakings outside the Union creating AI models could disregard the principle of 'privacy by design' laid down by Article 25 of the GDPR, or fail to build in European personal data protection standards from the design stage.

More than an application of extraterritoriality, this position of the European Data Protection Board confirms the 'contaminating' effect of the GDPR's provisions which, together with the impossibility for digital actors to forgo the European market, makes it possible to encourage, if not to compel, the building-in, from the design stage, of the European imperatives of personal data protection in data circulation. Through the authorities responsible for personal data protection, European law thereby asserts its determination to protect the personal data of European nationals in full, both within and beyond the borders of the European Union.

The challenges raised by AI are nonetheless pushing the European Union to reconsider its model, centred on personal data protection, in favour of one more conducive to the competitiveness of European actors.

2. Economic competition and the retreat from European principles: a model under strain

Until early 2025, there was no room for doubt as to the position of the European Union on data protection in the face of the demands of competitiveness.[185] It proposed at that time a third way between the United States conception of 'winner takes all'[186] through a deregulated development and the more 'Orwellian' Chinese conception.[187] In the race for AI, however, the European Union appears to be shifting its initial positions so as not to be left behind, technologically and economically alike. In other words, it would gradually abandon a model centred on the protection of fundamental freedoms for one geared to economic interests. Although this change of course is not yet settled, a number of signs point in that direction.

On 4 September 2025, the Court of Justice of the European Union, in its '*CRU*' judgment[188] , initiated a change of course. Although it reaffirms by this decision its constant jurisprudence,[189] it also opens the way to a potential challenge to the notion of personal data as currently defined. In concrete terms, among data relating to individuals, only anonymised data, which are not personal data, fall outside the personal data protection re-

185 Tifine, P. and Van Daal, L., "La circulation des données au service de l'intelligence artificielle", *RFDA* 2025, Dalloz, p. 6.

186 Marty, F., *Économie de la donnée : Écosystèmes numériques, algorithmes et intelligence artificielle, L'émergence d'un droit des données*, 2023, p. 35.

187 Castets -Renard, C., "Quelle politique européenne de l'intelligence artificielle ?", *RTD eur.*, 2021, p. 300-301.

188 CJEU, 4 Sept. 2025, C-413/23, *Contrôleur européen de la protection des données c/ Conseil de résolution unique (CRU)*. See: Ducluseau, E., "Transfert de données pseudonymisées à des tiers", *AJDA* 2025, n° 31, Dalloz, p. 1575; Biscarrat, M., "Transfert de données pseudonymisées à des tiers : la CJUE précise la portée de la notion de « données à caractère personnel", *JCP A* 2025, n° 37, LexisNexis, act. 424, p. 9; Bonneville, P., Iljic, A.,Lepka, E., Briançon, E. (chron.), "Notion de donnée à caractère personnel", *AJDA* 2025, n° 41, Dalloz, p. 2153; Martial-Braz, N., "Notion de donnée à caractère personnel – La construction prétorienne de la notion de donnée à caractère personnel : entre affirmation personnaliste et approche relative", *CCE* 2025, n° 10, LexisNexis, comm. 89, p. 40; Douville, T., "La notion de données à caractère personnel après l'arrêt CRU", *RTDcom* 2025, n°4, Dalloz, p. 1019.

189 CJEU, 20 Dec. 2017, case n° C-434/16, *Peter Nowak c/ Data Protection Commissioner*.

gime. The same is not true of pseudonymised data, which are personal data and to which the law of personal data protection applies. The novelty of this decision lies in calling into question the personal character of such pseudonymised data. In the guise of pragmatism, the CJEU holds that these data remain personal data for the data controller who, *de facto*, has the means to re-identify the person concerned, but that the same data may no longer be regarded as personal data by the third parties to whom they are disclosed, provided those third parties lack the means to carry out such re-identification. A third party's capacity for re-identification is then assessed by reference to the 'means reasonably likely to be used'.[190] These means are to be understood broadly: they may consist in existing technological means, or in the possibility of resorting to additional information.[191] The risk, therefore, is that pseudonymised data fall outside the law of personal data protection as soon as the holder lacks the means to re-identify the individuals to whom they relate. In its *Criteo* jurisprudence of 4 March 2026,[192] the *Conseil d'*État clarified this notion of reasonable means, holding that they were to be understood as 'not entailing a disproportionate effort in terms of time, cost and labour' and 'such that the [re] identification would be of no benefit [to the data controller]'.[193]

The CJEU's '*CRU*' decision will be welcomed by personal data practitioners, who will doubtless see in it a simplification and an alignment of the law with practice. This is all the more so for the data protection officers (DPOs) of the public administration, who process and collect data in order to carry out a public service mission rather than for commercial ends. This new interpretation, which removes pseudonymised data from the law of personal data protection, will undoubtedly ease procedures. The rejoicing may, however, be short-lived, given how significant a step backwards for personal data protection this decision represents. The short-term view, which sees in it a step forward through attention to practical concerns, could give way to the bitter realisation of a lasting inroad into the protection of privacy. The difficulty of monitoring the means of re-identification available to third-party data holders threatens to create a major risk for the protection of personal data. Moreover, there is nothing to suggest that the new course taken by the CJEU will not have the opposite effect, with data controllers taking greater precautions when transferring data to third parties so as to guard against any risk of re-identification by them, which would, in turn, add once more to their burden.

The debates are particularly lively between those who welcome this decision of the CJEU and those who fear it as a step backwards for personal data protection.[194] But the real turning point for the European conception of data came with an announcement of 19 November 2025,[195] with the publication of the 'digital omnibus' package, together with

190 Douville, T. (2025), La notion de données à caractère personnel après l'arrêt CRU, op. cit.

191 Ibid.

192 Conseil d'État, 4 March 2026, n° 482872, *Criteo*. See: Moussier, P., "Données pseudonymisées et RGPD : le Conseil d'État confirme l'approche de la CNIL", *Dalloz actualité*, 18 March 2026. Available at: https://www.dalloz-actualite.fr/flash/donnees-pseudonymisees-et-rgpd-conseil-d-etat-confirme-l-approche-de-cnil (consulted on 19 June 2026).

193 Ibid, recital n°12.

194 Draghi, M., "L'avenir de la compétitivité européenne – Partie A - Une stratégie de compétitivité pour l'Europe", *report to the European Commission*, 2024, p. 77.

195 Press release of European Commission, "Simpler EU digital rules and new digital wallets to save billions for businesses and boost innovation", Brussels on 19 Nov. 2025. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2718 (consulted on 19 June 2026).

a new data strategy.[196]

As regards this new strategy,[197] it pursues the objectives of innovation and AI development, now a priority of the European Union, which seeks to support the growth of undertakings in this sector while preserving the gains made by the Data Act and the Data Governance Act.

The digital omnibus package comprises three proposed regulations: the first is a draft regulation on digital wallets for undertakings[198] (Business Wallet), which is of no relevance to this study; the second, the digital AI omnibus,[199] essentially defers the entry into force of the provisions on high-risk AI systems laid down by the regulation on artificial intelligence (AI Act) and is likewise of no particular relevance to this study; finally the third, the digital omnibus regulation,[200] contains general measures relating, among other things, to European data law and is of major importance.

This last proposed regulation notably gives effect to the impact of the CJEU's *CRU* decision on pseudonymised data by proposing to amend the definition of personal data in Article 4 of the GDPR,[201] thereby confirming the link between the impact of this decision and the European Union's new direction. To this is added the introduction into the GDPR of an Article 88 *quater* (Article 88c), which establishes a legitimate interest in processing personal data for the development and operation of an AI system.[202] This objective of developing and operating AI could also create a new exception to the principle prohibiting the processing of so-called 'sensitive' personal data under Article 9 of the GDPR.[203] Article 12(5) of the GDPR, which allows a reasonable fee to be charged or processing to be refused where a data subject's request for information or access is manifestly unfounded or excessive, is supplemented by a new provision allowing the data controller to treat such a request as 'abusive'.[204] The CJEU was quick to draw on the proposed regulation here, acknowledging, in its *Brillen Rottler* decision of 19 March 2026,[205] the abusive character of an access request made by artificially [cre-

196 Communication from the Commission to the European Parliament and the Council «Data Union Strategy – Unlocking data for AI», COM(2025) 835 final, 19 Nov. 2025.

197 See Petel, A., "Que prévoit la stratégie pour une Union des données ?", *Dalloz actualité*, 3 Feb. 2026. Available at: https://www.dalloz-actualite.fr/flash/que-prevoit-strategie-pour-une-Union-des-donnees (consulted on 19 June 2026).

198 Proposal for a Regulation of the European Parliament and of the Council on the establishment of European Business Wallets, Brussels 19 Nov. 2025.

199 Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI).

200 Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus).

201 Ibid, article 3.

202 Ibid.

203 Ibid.

204 Ibid.

205 CJEU, 19 March 2026, case n° C-526/24, *Brillen Rottler*. See on this case: Loiseau, G., "Le droit d'accès aux données à caractère personnel recadré", *La Semaine Juridique Social (JCP S)*, 7 April 2026, n° 14, LexisNexis, reference point n°1118, p. 26.

ating] the conditions required to obtain an advantage under Article 12(5) of the GDPR. Furthermore, Article 33 of the GDPR, which sets out the procedure to be followed in the event of a data breach, is substantially relaxed to the detriment of personal data protection:[206] it now introduces a risk threshold for data breaches that must be notified, the notification having to be made within 96 hours rather than the 72 hours required under the law as it currently stands. These latter provisions may also be seen as a form of pragmatism, of alignment with practice, given that cyberattacks, phishing attempts and other ransomware are increasingly frequent and that the data stolen are not always of critical importance. The fact remains that, by placing data breaches considered to present a moderate risk outside this procedure, a weakening of the general regime of personal data protection is unavoidable.

Broadly, the digital omnibus regulation provides for a regulatory simplification and rationalisation intended to make the Data Act the vehicle for an expanded law of data, by which we mean a text that would govern personal, public and private data alike.[207] This drive towards simplification and rationalisation gives pause for thought: on the one hand, because it more closely resembles a deregulation proposal; on the other, because that deregulation rests essentially on considerations of competitiveness and innovation. The European Union is thereby moving away from its original model, from the principled position it had hitherto held, centred on the protection of individuals while attentive to the needs of economic actors and to innovation, towards a model close to that of the United States, but without the Big Tech.

Certain concerns have been formulated with regard to this new orientation, in the image of the Centre for European Policy Studies (CEPS), which warns against the EU's inclinations towards deregulation,[208] or that of the Centre on Regulation in Europe (CERRE), which, without denying the possible benefits of the digital omnibus package, deplores the notable absence of a global strategy on the part of the Commission. Mr Schnurr writes on this subject: 'But how these initiatives will meaningfully address Europe's challenges remains vague. In particular, fundamental questions remain about the Data Union

206 Article 3 of proposal for a digital omnibus.

207 To this end, the Digital Omnibus Regulation proposes to amend: the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR), Regulation (EU) 2018/1724 establishing a single digital gateway to provide access to information, Regulation (EU) 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (e-privacy Directive), Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 directive), Directive (EU) 2022/2557 on the resilience of critical entities (RCE Directive).

But also to repeal: Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union (FFoD), Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services (P2B regulation), Regulation (EU) 2022/868 on European data governance and amending Regulation (Data gouvernance act), Directive (EU) 2019/1024 on open data and the re-use of public sector information (open data directive).

208 Thomadakis, A., "The EU is walking a fine line between simplification and deregulation", 13 Oct. 2025. Available at: https://www.ceps.eu/the-eu-is-walking-the-fine-line-between-simplification-and-deregulation/ (consulted on 19 June 2026).

Strategy's goal of 'scaling up access to quality data for AI and innovation'.[209] Since these European proposals bring more new questions than answers, he concludes upon these three essential questions: 'What incentives will businesses have to share their data, given their concerns about trade secrets, privacy, and competition, as the Commission itself acknowledges? How will unlocking data for AI deliver concrete benefits for European businesses and consumers, while not fuelling market concentration? How can AI Gigafactories and other flagship initiatives support organisations to develop sustainable business models capable of competing with global players over the long term?'. On this last point, it would seem that a beginning of an answer consists in acknowledging that to undertake a policy of deregulation without being oneself endowed with 'global players' appears to constitute a high-risk strategy.

Finally, certain bodies of the European Union have been able to formulate certain criticisms of the digital omnibus package. First, the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) adopted a joint opinion on the proposed digital omnibus regulation which, while welcoming the proposal, contests certain provisions. They oppose notably the provisions relating to the modification of the definition of personal data, which 'would also result in a more restrictive interpretation of the concept of personal data, limit the scope of application of the GDPR, and thus negatively affect the protection of the fundamental rights and freedoms of individuals while increasing legal uncertainty for organisations'.[210] As regards Article 88 *quater* (Article 88c) which grounds a legitimate interest for the processing of personal data with a view to the development and the exploitation of an AI system, the EDPB recalls that it has already explicated this point in a previous opinion,[211] and that 'it is not necessary to add a specific provision to the GDPR on this point'. In the same manner, the Internal Market and Consumer Protection (IMCO) Committee has commissioned a study[212] on the subject by which it warns concerning the nature of the digital omnibus, which is not limited to a technical simplification and a harmonisation of the law and could engender a substantial weakening of individuals' rights.

209 Schnurr, D., "The digital omnibus: positive steps, but unclear strategy, News & Insights on CERRE website", 28 Nov. 2025. Available at: https://cerre.eu/news/the-digital-omnibus-positive-steps-but-unclear-strategy/ (consulted on 19 June 2026).

210 EDPB-EDPS Joint opinion 2/2026 on the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus), point n° 21, p. 11. Available at: https://www.edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-22026-proposal_en (consulted on 19 June 2026).

211 EDPB Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models, adopted on 17 Dec. 2024, Section 3.3. Available at: https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_en (consulted on 19 June 2026).

212 Skiotytė, G., Sadauskaitė, A., "A Digital Omnibus: Identifying Interlinks and Possible Overlaps Between Different Legal Acts in the Field of Digital Legislation to Streamline Tech Rules", European Parliament, Policy Department for Economy and Growth, 2026. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2026/772641/ECTI_STU(2026)772641_EN.pdf (consulted on 19 June 2026).