LUISS

School of Government

The digital omnibus: towards a systematic architecture of the eu digital acquis

a cura di **Sofia Palascino**
Collaboratrice del progetto di ricerca "AIDEAL:
AI for Decision-making in Effective and Accountable Leadership"

Working Paper Series
SOG-WP04/2026
ISSN: 2282-4189

LUISS SCHOOL OF GOVERNMENT

ABSTRACT

The 'Digital Omnibus' package, presented by the European Commission on 19 November 2025, was formally characterised as an administrative simplification measure. The central thesis advanced here is that the Omnibus does not merely streamline the Union's digital acquis but repositions its normative centre of gravity, shifting the framework's primary orientation toward the promotion of market efficiency, regulatory competitiveness, and risk-based governance. Three dimensions of this shift are examined in detail: the consolidation of European data regulation around an expanded Data Act, and the axiological implications of relocating the Data Governance Act's fiduciary governance logic within a market-integration framework; the proposed redefinition of the notion of personal data in Article 4(1) GDPR, which would transform identifiability from an objective criterion into a controller-relative assessment, with direct consequences for the uniformity of data subjects' protection; and the reconfiguration of procedural rights, including the right of access and the consent model for AI training data. The article further contends that the competitiveness rationale invoked to support these changes rests on an empirically fragile causal premise that the Commission has not substantiated. In the concluding section, the article argues that the constitutional coherence of the revised acquis will depend substantially on the supervisory and adjudicative role of the Court of Justice of the European Union.

Keywords: Digital Omnibus, European digital acquis, personal data, fundamental rights.

1. THE EUROPEAN CONTEXT

Over the past five years, the European Union has undergone an intensive period of legislative activity in the digital domain. Between 2019 and 2024, instruments of systemic significance were adopted, including the GDPR, the AI Act, the Data Act, the Data Governance Act, and the NIS2 and DORA Directives.[1] With that wave of regulatory expansion now largely concluded, the European legislature appears to be turning toward a different objective: not the multiplication of legal instruments, but their rationalisation, coordination, and the reduction of the compliance costs generated by their accumulated layers.

This new direction has been significantly shaped by the Draghi Report on European Competitiveness and by the Commission Communication "A simpler and faster Europe".[2] Within that framework, the Commission has described the new regulatory season as a physiological reversal of the trend toward the normative accumulation of previous years.[3] This characterisation captures a genuine dimension of the phenomenon, but does not exhaust its significance: the transition from the production of new rules to the rationalisation of existing ones is not, in substantive terms, an axiologically neutral operation, and cannot be subsumed entirely under the category of administrative simplification.

It is within this context that the 'Digital Simplification Package' – presented on 19 November 2025 and commonly referred to as the Digital Omnibus – must be situated. The package comprises two interconnected legislative proposals. The first amends the GDPR and the ePrivacy Directive, principally with regard to the consent regime for cookies and the rules governing pseudonymised data. The second makes targeted modifications to the AI Act, including, inter alia, the deferral of certain application deadlines for high-risk systems.[4] Taken together, the two proposals present themselves as an attempt to bring coherence to a digital acquis characterised by overlapping provisions, interpretive friction, and compliance costs that the Commission considers no longer sustainable.[5]

The Commission situates the initiative within its Better Regulation agenda, justifying the absence of a standalone impact assessment on the grounds that the modifications introduced are merely targeted and technical, aimed at making the implementation of existing rules more efficient.[6] It is precisely this formal framing, however, that requires careful analytical scrutiny. Once examined closely, several of the proposed changes operate not at the level of administrative machinery but at the level of fundamental legal categories and structural rights guarantees. For this reason, the Omnibus must be analysed not only as a technique of regulatory coordination, but as a potential factor in redefining the normative orientation of European digital governance – a process that, however incremental in appearance, carries implications that the 'simplification' register does not adequately capture.

---

1 R. KOCH, T. WECK, A. DIEFENHARDT et al., Policy Briefing: A Strategic Analysis of the EU's Digital Omnibus Package, Frankfurt School, 2026, p. 1.
2 European Commission, Proposal for a Regulation of the European Parliament and of the Council as regards the simplification of the digital legislative framework (Digital Omnibus), 19 November 2025.
3 M. GARTNER, The Digital Omnibus on AI: First Analysis of the EU's Policy Pivot on the AI Act, in Journal of AI Law and Regulation, vol. 4, 2025, p. 1.
4 D. KORFF, Digital Omnibus: proposed changes to the definition of personal data in the EU GDPR analysed in the light of the SRB and earlier CJEU judgments, in SSRN Electronic Journal, 2026, p. 2; K. SUZUKI, Privacy Enhancing Technologies in the EU Digital Omnibus Proposal: Clarifying the Role of PETs in the Definition of Personal Data under the GDPR, paper, 2026, p. 11.
5 O. POLLICINO, F. PAOLUCCI, Col Digital Omnibus l'Europa può smarrire sé stessa, in Agenda Digitale, 2025, p. 3.
6 European Commission, Proposal for a Regulation, cited above, 19 November 2025.

2. TOWARDS A MORE UNIFIED DIGITAL ARCHITECTURE

One of the most significant aspects of the Digital Omnibus concerns the comprehensive reorganisation of European data regulation. The proposals provide for the repeal of the Data Governance Act, the Open Data Directive, and the Free Flow of Non-Personal Data Regulation, with the simultaneous transfer of their substantive regulatory apparatus into a structurally expanded Data Act.[7] Into that expanded framework are channelled, in particular, the regime governing data intermediation services, the mechanisms for data altruism, and the rules on the reuse of public sector information. In the same vein, the P2B Regulation is to be repealed, on the basis that the majority of its protective functions are now considered absorbed by the DSA and DMA's scope of application.[8]

This operation is not, however, equivalent to a mere reduction in the number of legal sources. It signals a precise direction of regulatory policy: the Data Act is being positioned as the structural axis of European data regulation, concentrating within itself an ever-greater share of the relevant governance functions.[9] The question at issue is not, in other words, simply quantitative but qualitative: which act becomes the gravitational centre of the system, and with what normative orientation it exercises that function.

In this regard, the reabsorption into the Data Act of the institutions originally established by the Data Governance Act merits specific attention. The DGA gave normative weight to a governance logic in which data intermediation and data altruism were conceived not merely as instruments for the circulation of information, but as mechanisms for reliability, accountability, and the protection of data subjects and the wider public interest.[10] More concretely, the DGA imposed a strict neutrality obligation on data intermediaries – prohibiting them from processing data for purposes beyond the intermediation service itself – and required data altruism organisations to operate on a not-for-profit basis, reflecting a deliberate legislative choice to place certain data-sharing activities outside purely commercial governance.[11] It is in this sense that one may speak of an original fiduciary and institutional model: a model in which certain intermediaries operate not as mere facilitators of economic exchange, but as custodians of interests that transcend the logic of market efficiency alone.[12]

With their reabsorption into the Data Act, those functions do not formally disappear,

7 B. LAZAROTTO, The Data Omnibus: The Good, the Bad, and The Ugly Behind the DGA and Data Act, in MediaLaws Blog, 2025, pp. 1–2.

8 On the relationship between the P2B Regulation and the subsequent DSA/DMA framework, and on the progressive absorption of platform-to-business protective functions into the broader EU platform regulation architecture, see I. GRAEF, Why End-User Consent Cannot Keep Markets Contestable: A Suggestion to Strengthen the Limits on Personal Data Combination in the Proposed Digital Markets Act, in Verfassungsblog, 2021, p. 22; and G. DE GREGORIO, P. DUNN, The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age, in Common Market Law Review, 2022.

9 A. F. URICCHIO, C. CALDAROLA, Verso un ecosistema digitale europeo integrato. Digital Omnibus, Data Act, AI Act e tutela della persona umana nella governance dei dati e dell'Intelligenza Artificiale, in Culture Digitali, 2026, pp. 8–9.

10 B. MARTENS, The European Union needs more than the digital omnibus to make digital services competitive, in Bruegel, 2025, p. 5.

11 Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance (Data Governance Act), Arts 12(a) and 18(1). Article 12(a) prohibits data intermediaries from using the data shared with them for purposes other than making it available to data users; Article 18(1) requires data altruism organisations to be established as non-profit entities. These structural constraints embodied a specific governance logic that is not replicated by the Data Act's framework, which is primarily oriented toward B2B data sharing and the reduction of switching and interoperability barriers.

12 The term "fiduciary" is used here in a structural rather than strictly private-law sense, to describe an arrangement in which an intermediary is entrusted with data subject to obligations of loyalty toward the data principal rather than toward its own commercial interests. For an influential account of the fiduciary model applied to data intermediaries, see J.M. BALKIN, Information Fiduciaries and the First Amendment, in UC Davis Law Review, 2016, p. 1183, where the author argues that enterprises managing personal information in ways that create structural dependency warrant fiduciary-type constraints.

but are relocated within a framework whose primary orientation is toward the facilitation of B2B data sharing, cloud interoperability, and the reduction of vendor lock-in. The DGA's neutrality requirement and non-profit condition are no longer embedded in a governance instrument designed around public interest data sharing; they become elements of a broader market-integration statute whose teleological centre lies elsewhere. The risk lies not in the immediate abolition of these protective logics, but in the gradual erosion of their ordering force: once removed from the institutional framework that gave them their normative purpose, they become subject to interpretive pressures that the market-integration rationale of the Data Act is ill-equipped to resist.

For this reason, the consolidation underway cannot be characterised as axiologically neutral. It alters the systemic context within which instruments that, in the previous regulatory architecture, derived their legitimacy more explicitly from considerations of fiduciary mediation, institutional accountability, and the public interest, are now situated. Regulatory consolidation of this kind has been observed, in comparative perspective, to reduce the distinctiveness of protective governance frameworks when the absorbing instrument reflects a structurally different normative hierarchy — a risk the Omnibus does not adequately address.[13]

An analogous rationalisation is apparent, through different means, on the artificial intelligence front. The proposed amendments to the AI Act introduce a recalibration of the timetable for applying the obligations relating to high-risk systems, making their operability contingent on the concrete availability of harmonised technical standards, guidelines, and support instruments.[14] The regime thus shifts from one of fixed deadlines to one that is more closely tied to the readiness of the technical and applicative framework.

This temporal recalibration is accompanied by a more pronounced institutional centralisation: supervisory powers over general-purpose AI models, and over AI systems integrated into Very Large Online Platforms and Very Large Online Search Engines, are to be concentrated in the AI Office.[15] The stated objective — reducing applicative fragmentation and ensuring greater uniformity of supervision — is in principle intelligible. It remains to be assessed, however, whether this simplification of the governance level may produce, in terms of the effective protection of those concerned, a growing distance between the institutional site of regulation and the practical exercise of remedies.

13 H.C.H. HOFMANN, This Is Not Simplification: How to Simplify the Digital Acquis Without Undermining Rights, in Verfassungsblog, 2026, p. 3.
14 European Commission, Proposal for a Regulation, cited above, p. 84.
15 On the institutional architecture of the AI Act and the governance role of the AI Office, with particular reference to the supervision of general-purpose AI models and of systemic risks, see M. VEALE, F. ZUIDERVEEN BORGESIUS, Demystifying the Draft EU Artificial Intelligence Act, in Computer Law Review International, 2021, p. 97; and N.A. SMUHA, et al., How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act,LEADS Lab, University of Birmingham, 2021, particularly Part IV on enforcement and supervisory design

3. THE REDEFINITION OF PERSONAL DATA AND THE RECONFIGURATION OF PROCEDURAL RIGHTS

Perhaps the most doctrinally significant dimension of the Digital Omnibus concerns the amendments to the GDPR. It is here that the distance between the Commission's formal characterisation of the intervention as "technical" and its actual significance at the dogmatic level becomes most apparent.

The proposed amendment to Article 4(1) GDPR, relating to the notion of personal data, provides an exemplary illustration. Under the approach underpinning the Omnibus, identifiability would no longer be assessed in predominantly objective terms, but would instead be made more dependent on the position of the individual controller. From this perspective, information could cease to qualify as personal data in relation to a given entity if that entity does not possess the means reasonably likely to be used to identify the data subject, irrespective of whether other actors in the processing chain may hold such means.[16]

Formally, the Commission characterises such an amendment as technical, since it operates on a definitional provision. In substantive terms, however, the matter is considerably more complex. The redefinition of the identifiability criterion bears on the threshold at which the protections afforded by the GDPR are triggered: it does not merely regulate the application of a legal category more precisely, but alters its operational meaning in a structurally significant way.[17] The same information could qualify as personal data for one operator while not qualifying for another, with inevitable consequences for legal certainty and for the uniformity of the protections afforded to data subjects.[18]

Beyond the legal certainty concern, the proposed amendment raises a direct proportionality question under Article 52(1) of the Charter of Fundamental Rights of the EU, which conditions any limitation on a Charter right on respect for its essential content and on satisfaction of the necessity and proportionality requirements. The right to personal data protection under Article 8 CFR attaches to data as an objective legal category, not as a function of the controller's technical position[19]. A controller-relative redefinition of what counts as personal data effectively narrows the material scope of the right – a form of limitation that, under the Court's established jurisprudence, requires the legislature to demonstrate that it genuinely meets a public interest objective and does not exceed what is strictly necessary to achieve it. The Commission's characterisation of this amendment as "targeted and technical in nature", and its consequent exemption from a standalone impact assessment, does not discharge that constitutional obligation.

It is for this reason that the distinction between a technical intervention and one carrying ontological significance must be articulated with precision: an amendment to the definition of personal data is never merely a definitional matter; it produces effects

16 On the structural ambiguity of the notion of identifiability and the risks associated with a controller-relative reading of Article 4(1) GDPR, see N. PURTOVA, The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law, in Law, Innovation and Technology, p. 40.

17 R. MAHIEU, The Ominous Omnibus: Dismantling the Right of Access to Personal Data, in Verfassungsblog, 2025, p. 3.

18 A. ALEMANNO, The Omnibus Road to Constitutional Drift: How the Rise of Omnibus Legislation Undermines Procedural Integrity in the EU, in Verfassungsblog, 2025, p. 1.

19 With specific reference to data protection and the constitutional discipline governing limitations of Article 8 CFR, see O. LYNSKEY, The Foundations of EU Data Protection Law, in Oxford University Press, 2015, pp. 156–178.

that run through the entire operational architecture of the regulation.[20]

This redefinition is accompanied by a parallel reconfiguration of data subjects' procedural rights, and in particular of the right of access. The proposed amendment to Article 12(5) GDPR permits controllers to refuse manifestly unfounded or excessive access requests – or to subject them to a reasonable fee – including where those requests are considered unrelated to the genuine protection of personal data.[21] The mechanism is accompanied by a relaxation of the evidential burden on the controller: establishing reasonable grounds for presuming the excessive character of the request is held to suffice.[22]

There is no doubt that the legal order has a legitimate interest in preventing abusive uses of the right of access. The constitutional difficulty, however, lies in the specific design of the restriction. The right of access has not operated merely as an informational tool; as confirmed by the Court of Justice, it is an instrument through which data subjects exercise control over their personal sphere, surface informational asymmetries, challenge opaque processing operations, and verify the functioning of automated decision-making.[23] The introduction of an "instrumental purpose" exclusion – permitting refusal where requests are unrelated to the protection of personal data stricto sensu – risks immunising a wide range of commercially sensitive processing from access-based scrutiny precisely because the data subject's motivation extends beyond data protection in the narrow sense: workers seeking to audit algorithmic management systems, consumers challenging profiling practices, and citizens verifying AI-assisted administrative decisions all necessarily pursue purposes that transcend the narrow protection of personal data in the abstract. The proposed exclusion, read broadly, would deprive the access right of much of its accountability function – an outcome that is difficult to reconcile with the right's constitutional basis in Articles 7 and 8 CFR.[24]

A still more significant transformation concerns the processing of data for the training of artificial intelligence systems. The insertion of new Article 88-quater into the GDPR would position legitimate interest as the primary legal basis for processing personal data for AI development purposes, in lieu of the traditional consent model, which would be replaced by an opt-out mechanism.[25] An analogous opening is envisaged, under certain conditions, for special categories of data as well.

The normative significance of this shift cannot be reduced to a question of compliance costs. The distinction between consent and legitimate interest is not merely procedural but structural: it determines who bears the default burden in the controller–data subject relationship. Consent makes processing impermissible as a matter of principle unless the data subject has affirmatively authorised it; it positions privacy as the regulatory baseline and commercial exploitation as the exception that requires justification. Legitimate interest inverts this structure: it positions processing as permissible by default, subject to a balancing exercise that the controller conducts and that the data subject can only resist through subsequent objection.[26] The opt-out

20 B. LAZAROTTO, cited above, p. 4.
21 F. BIEKER, K. NOLAN, European AI FOMO: The European Commission Sacrifices the Digital Acquis at the Altar of AI Hype, in Verfassungsblog, 2026, p. 3.
22 H. A. KURTH, EU Digital Omnibus Introduces a Single Reporting Point for Cybersecurity Incidents, in Privacy & Cybersecurity Law Blog, 2025, p. 3.
23 see R. MAHIEU, The Right of Access to Personal Data: A Genealogy, in Technology and Regulation, 2021, particularly Chapters 4–6.
24 M. GARTNER, cited above, p. 3.
25 European Commission, Proposal for a Regulation, cited above, 19 November 2025.
26 EDPB and EDPS, Joint Opinion 2/2026 on the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus), 10 February 2026, p. 9, expressing serious concern that the proposed legitimate interest basis for AI training processing may not provide an adequate level of protection equivalent to that which the consent framework has historically ensured.

mechanism preserves formal individual agency, but it does so residually and reactively rather than structurally and proactively – a difference that matters particularly in contexts where data subjects are systematically uninformed about the purposes for which their data is processed. This does not mean that legitimate interest can never be an appropriate basis for AI training; but it does mean that establishing it as the default and general basis for an entire category of commercially significant processing requires a constitutional justification proportionate to the resulting displacement of data subjects' control.[27]

The "disproportionate effort" clause – which permits a controller to refrain from deletion where compliance would require the redesign or retraining of the entire AI model – only partially mitigates this concern. It addresses the operational difficulty of post-hoc erasure but does not respond to the prior question of whether processing should have been permitted in the first place, nor to the structural accountability deficit created by the default permissibility of the processing.

4. EFFICIENCY, COMPETITIVENESS, AND THE LIMITS OF THE SIMPLIFICATION RATIONALE

A full understanding of the Omnibus requires consideration of the broader strategic context within which it is embedded. The initiative does not simply rationalise the digital acquis; it is situated within a more general reflection on Europe's competitiveness in the technology sector, shaped decisively by the Draghi Report's diagnosis of regulatory overload as a structural impediment to European technological development.[28] In that context, the vocabulary of simplification is systematically coupled with that of efficiency, innovation, and the Union's capacity to compete with the world's leading digital powers.[29]

Part of this approach identifies a real and legitimate concern. European digital law has become, over time, complex, layered, and costly to apply, particularly for smaller operators. The Commission's aim of reducing administrative burdens and constructing a more coherent and accessible regulatory framework is therefore not without foundation.[30] Some of the Omnibus's measures move coherently in this direction: the establishment of a single access point for cybersecurity incident notifications, the extension of certain exemption regimes to small mid-caps, the introduction of European Business Wallets, and the restriction of certain Business-to-Government data-sharing obligations are, in principle, legitimate objectives of operational rationalisation.[31]

The difficulty arises, however, when the rationalisation of those aspects is invoked as a general justification for interventions that bear on fundamental concepts of the GDPR or on the level of protection afforded to certain rights. That reducing compliance costs is a legitimate objective is scarcely contestable. Less evident is that this objective alone is sufficient to justify the redefinition of the notion of personal data, the restriction of

27 R. BECKER, E.S. DOVE, The EU GDPR and secondary use of health and genetic data for research support purposes, in International Data Privacy Law, 2026, pp. 1–2.
28 O. POLLICINO, F. PAOLUCCI, cited above, p. 6.
29 M. Gartner, cited above, p. 3.
30 H. RUSCHEMEIER, The Omnibus Package of the EU Commission: Or How to Kill Data Protection Fast, in Verfassungsblog, 2025, p. 7.
31 R. KOCH, T. WECK, A. DIEFENHARDT et al., cited above, p. 5.

the right of access, or the replacement of consent with legitimate interest in the regime governing AI training data processing.[32]

The Omnibus appears to presuppose a direct causal link between the stringency of the EU data protection framework and Europe's relative underperformance in generating global technology leaders. This causal premise deserves scrutiny, because the strength of the justification for the most constitutionally sensitive measures in the package depends directly on its empirical validity. Empirical and comparative scholarship has shown the competitive gap between European and American technology ecosystems is attributable in decisive measure to structural factors that are distinct from regulatory stringency: the fragmentation of the digital single market, which prevents the achievement of the scale necessary to compete with US and Chinese platforms; the underdevelopment of European venture capital markets; insolvency regimes that impose costs on business failure disproportionate to those in the United States; and systemic disadvantages in attracting global talent.[33] These structural conditions – not data protection law – are the primary determinants of Europe's technological disadvantage. Moreover, the EU's regulatory stringency has historically generated a 'Brussels Effect', positioning Europe as a global standard-setter whose rules shape compliance behaviour well beyond its borders: a capacity that depends precisely on the distinctiveness and coherence of its regulatory model.[34]

5. LEGAL UNCERTAINTY AND THE IMPACT ON THE EUROPEAN PRODUCTIVE SECTOR

The Omnibus also raises two distinct orders of concern that are best addressed separately.

The first relates to legal certainty. Paradoxically, a package designed to simplify the digital acquis risks generating, in certain of its segments, new areas of normative indeterminacy[35]. This arises in particular where the substantive content of obligations is referred to technical standards yet to be adopted, to open-ended general clauses, or to heavily context-dependent assessments left to the controller's own discretion.[36] Such an arrangement increases the system's flexibility, but simultaneously makes it more difficult to determine ex ante the concrete level of protection required or the degree of compliance demanded – with attendant uncertainty effects that may prove more burdensome than the compliance costs the simplification sought to eliminate[37]. The

32 K. FAISAL, The Digital Omnibus and the Future of EU Digital Governance: Simplification or Strategic Dilution?, in EU Law Live, 2026.

33 A. BRADFORD, The False Choice Between Digital Regulation and Innovation, in Northwestern University Law Review, vol. 118, no. 2, 2024, available at SSRN: https://ssrn.com/abstract=4753107. Bradford demonstrates that Europe's competitive disadvantage in generating global technology leaders is attributable in decisive measure to structural market conditions – the fragmentation of the digital single market, the underdevelopment of venture capital, restrictive insolvency regimes, and talent attraction deficits – rather than to regulatory stringency. If this structural diagnosis is correct, the Omnibus's most constitutionally sensitive measures are not proportionate means of achieving the competitiveness objective they invoke: they impose real rights costs in pursuit of a causal theory that the evidence does not support. The causal premise therefore fails not merely as an empirical matter but as a constitutional justification.

34 A. BRADFORD, The Brussels Effect: How the European Union Rules the World, New York, Oxford University Press, 2020, pp. 25–60, developing the argument that the EU's regulatory influence operates through the market mechanism of intra-firm globalisation: the stringency of EU standards, combined with the size of the EU market, creates incentives for firms to adopt EU-standard practices globally rather than maintain dual compliance regimes.

35 On the paradox by which simplification initiatives may generate, rather than reduce, normative indeterminacy, see A. ALEMANNO, The Better Regulation Initiative at the Judicial Gate: A Trojan Horse within the Commission's Walls or the Way Forward?, in European Law Journal, p. 382; and C.M. RADAELLI, Whither Better Regulation for the Lisbon Agenda?, in Journal of European Public Policy, 2007, p. 190.

36 O. POLLICINO, remarks at the seminar 'La regolazione dell'intelligenza artificiale: il modello italiano nel quadro dell'AI Act Europeo', Università Luiss Guido Carli, 9 February 2026.

37 On the relationship between legal certainty, foreseeability and the rule of law in the EU legal order, see T. TRIDIMAS, The General Principles of EU Law, Oxford European Union Law Library, 2006, Chapter 6; and J. RAITIO, The Principle of Legal Certainty in EC Law, Springer, 2003.

delegation of definitional and applicative choices to implementing acts and technical standard-setting bodies, moreover, raises accountability concerns of its own: the further the normative content of rights obligations is removed from the legislative text, the harder it becomes for courts, supervisory authorities, and data subjects to hold controllers to clearly defined standards.

The second dimension concerns the Omnibus's distributional impact on the European productive sector. In the abstract, many of the package's measures aim to lighten the regulatory burden on smaller operators and to make the European market more dynamic[38]. In practice, however, a system that entrusts a significant portion of its operation to elastic evaluative standards and to verifications left to the controller's initiative is structurally inclined to favour operators who are better equipped in organisational and legal terms.[39] Large undertakings possess the internal resources to manage broad interpretive margins; most SMEs do not, in equivalent measure. For this reason, it is by no means certain that more flexible regulation will automatically produce a more equitable or more contestable market: regulatory flexibility, absent clear and enforceable minimum standards, tends to replicate existing market asymmetries rather than correct them.

6. CONCLUDING OBSERVATIONS: FUNDAMENTAL RIGHTS AND THE CONSTITUTIONAL INTEGRITY OF THE DIGITAL ACQUIS

Considered as a whole, the Digital Omnibus presents itself as an exercise in regulatory coordination, but its most significant provisions operate at a different level: they modify the definitional scope of a fundamental right, reconfigure the structural relationship between controllers and data subjects, and displace consent as the normative baseline for a class of commercially significant processing. These are not administrative adjustments; they are changes to the constitutional architecture of European data protection law, and they raise questions that the 'simplification' framing leaves systematically unaddressed[40].

The central question this article has sought to advance is the following: can changes of this kind be constitutionally justified by reference to administrative efficiency and competitive necessity? The analysis in the preceding sections suggests that the answer, on the basis of currently available evidence, is negative – at least in the absence of a proportionality assessment that the Commission has not conducted and that the framework of the Better Regulation agenda has not been designed to provide[41].

38 On the structural compliance disadvantage faced by SMEs under the GDPR and adjacent digital regimes, see G. Malgieri, J. Niklas, Vulnerable Data Subjects, in Computer Law & Security Review, 2020.

39 N. LUPO, remarks at the seminar 'La regolazione dell'intelligenza artificiale: il modello italiano nel quadro dell'AI Act Europeo', Università Luiss Guido Carli, 9 February 2026.

40 On the tension between "simplification" rhetoric and substantive fundamental-rights recalibration in EU digital regulation, see G. DE GREGORIO, Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society, Cambridge University Press, 2022, particularly Chapter 4. See also P. NEMITZ, Constitutional Democracy and Technology in the Age of Artificial Intelligence, in Philosophical Transactions of the Royal Society, 2018.

41 For a critical reconstruction of the Better Regulation agenda and its limits in capturing fundamental-rights trade-offs, see A. ALEMANNO, The Better Regulation Initiative at the Judicial Gate: A Trojan Horse within the Commission's Walls or the Way Forward?, in European Law Journal, 2009, p. 382.

Three specific constitutional questions will require resolution, whether in the legislative process or, ultimately, before the Court of Justice of the European Union. The first concerns the proposed controller-relative redefinition of personal data: whether a reduction in the material scope of the right to data protection under Article 8 CFR, effected through a definitional amendment that the Commission characterises as technical, satisfies the conditions of Article 52(1) CFR – in particular the requirements that limitations must be provided for by law, must respect the essential content of the right, and must be genuinely necessary and proportionate to a recognised objective of general interest[42]. The second concerns the restructuring of the right of access: whether the introduction of an "instrumental purpose" exclusion and the relaxation of the evidential burden can be reconciled with the access right's constitutional function as an accountability mechanism, as the Court has affirmed it to be. The third concerns the shift from consent to legitimate interest for AI training: whether a modification that structurally inverts the default allocation of control between controllers and data subjects – making large-scale commercial processing of personal data permissible by default, subject only to a reactive opt-out – is compatible with the right to informational self-determination that Articles 7 and 8 CFR protect[43].

It will fall to the Court of Justice to determine whether these new solutions are compatible with the level of protection that Union law requires, and with the conception of data protection as a safeguard of individual liberty, dignity, and self-determination[44]. The decisive question is not whether European digital law should be simplified – that it should be rendered more coherent and less burdensome is not in doubt – but within what constitutional limits such simplification can be achieved. Those limits are not self-executing; they require active judicial enforcement. The role of the Court will be not merely to correct legislative overreach after the fact, but to ensure that the restructuring of the digital acquis proceeds in a manner consistent with the foundational values upon which the Union's regulatory authority – and its global normative credibility – ultimately depends[45].

42 On Article 52(1) CFR and the structure of permissible limitations, see S. Peers, T. Hervey, J. Kenner and A. Ward (eds), The EU Charter of Fundamental Rights: A Commentary , Bloomsbury Publishing, 2021.

43 On consent as the structural baseline of EU data protection and the risks of its erosion, see B.-J. KOOPS, The Trouble with European Data Protection Law, in International Data Privacy Law, 2014, p. 250.

44 On data protection as a safeguard of dignity, autonomy and self-determination, see L.A. BYGRAVE, Data Privacy Law: An International Perspective , Oxford University Press, 2014, Chapters 6–7.

45 On the institutional role of the Court of Justice in safeguarding the constitutional integrity of the digital acquis, see G. DE GREGORIO, Digital Constitutionalism in Europe, Cambridge University Press, 2022, Chapter 6; and O. POLLICINO, Tutela dei diritti fondamentali nell'era digitale e contesto valoriale: una indagine transatlantica, in MediaLaws, 2018.

LUISS

School of Government

Via di Villa Emiliani, 14
00198 Roma Italia
T: 0039 06 8522 5096