

Beyond the 'Brussels effect'

December 2025

By Gautam Kamath and Chloe Teevan

Summary

This briefing note argues that the 'Brussels effect' is not dead but is evolving. Shifting geopolitics requires a change in the European Union's approach – moving from regulatory dominance to one of partnership with other global actors.

The EU's move to simplify its vast digital rulebook, exemplified by the EU's recent 'digital omnibus' simplification agenda, has been met with internal criticism as a potential rollback of digital rights. Meanwhile, proponents see it as a necessary step to reduce complexity and foster investment. Internationally, a pushback against the unidirectional force of the 'Brussels effect' was already apparent long before the so-called 'digital omnibus.' A growing number of countries – like India, Brazil, and Japan – are developing their own distinct digital regulatory frameworks. India has adopted a 'techno-legal' approach through its Data Empowerment and Protection Architecture (DEPA), and its focus on rolling out 'Digital Public Infrastructure' (DPIs) across different parts of the economy – payments, identity, e-commerce, energy grids, etc.

To remain relevant, the EU must also embrace this 'techno-legal' approach, as exemplified by the planned EU Digital Identity (EUDI) Wallet. It should also work with partners such as India, Brazil, and Japan to co-create open protocols and standards, transforming the 'Brussels effect' into a multinational 'third way' for digital governance.

Introduction

Europe's current regulatory approach may be [seeing the end of the road](#), as demonstrated by the so-called '[digital omnibus](#)' of 19 November 2025. Yet, it is essential that Brussels does not simply cede its regulatory power, but works to build something new in partnership with other global actors.

Part of that conversation is starting in national capitals, most notably with the [Franco-German Digital Sovereignty Summit](#) in Berlin on 18 November 2025, and in the [Eurostack Initiative](#)'s push for a European digital industrial policy.

Countries around the world are also having similar conversations about how to regulate the digital sector and tackle the dominance of a few large players. Indeed, the world needs forward-looking digital regulations to accompany disruptive future technologies.

In an age where there are increasingly two dominant digital superpowers – the United States and China – and where Europeans feel dominated by a handful of large tech companies, Brussels has a real interest in working with other global actors to build a forward-looking multinational coalition. Rather than bemoaning the death of the 'Brussels effect', it is more appropriate to see it as an evolution where Brussels will need to work with others on an equal footing as partners.

This is also why the European Commission's [International Digital Strategy](#) calls for a 'Team Europe' tech business offer, based on combining technologies in a modular way with partners 'to create a package of mutual benefits'. We need Europe to team up with the world, both on [technology](#) and on regulation.

Simplification or simple deregulation?

As the European Union institutions finalised the 'digital omnibus' package "to optimise the application of the digital rulebook," it has been met with strong reactions. On the one hand, critics see this as Brussels bowing down to Big Tech and the current US administration's agenda of deregulation, while proponents see it as a much-needed step in the 'simplification' of the EU's digital rulebook. There is no doubt that a review was much needed to fix the coherence and complexity of the EU digital acquis, although it is by no means clear yet if this has been achieved. Indeed, attempts to simplify regulation may be a distraction from the much more difficult task of making real advances [to complete the European Single Market](#).

Some highlights of the omnibus include a delay on obligations for high-risk AI providers (a [demand](#) made by European industry), changes to GDPR that allow AI providers to use legitimate interest to process personal data for AI-related purposes, and a single entry point for incident notification under various cybersecurity laws.

On privacy, allowing a review and streamlining of GDPR has positive implications for unseemly obstacles like persistent cookie banners, as well as more streamlined reporting requirements, and it also facilitates 'low impact' data processing, which includes training AI models. This might help reduce the burden on Data Protection Authorities (DPAs) across the EU, which are already under-resourced and would otherwise have to deal with a flurry of new cases, but it does not necessarily address new risks to data protection that emerge from widespread AI deployment. The new '[EU Data Union Strategy](#)' scales up the availability of high-quality data sets and data spaces to help European businesses train their own models. It also provides model clauses for cloud computing contracts and data access and use. There is a clear shift, where the European Commission has focused on removing obstacles for industry, while at the same time strengthening the investment and rollout of AI.

A group of [127 different civil society organisations firmly opposed it](#), viewing it as a Trojan horse to achieve deregulation. They have called it "an attempt to covertly dismantle Europe's strongest protections against digital threats" and "the biggest rollback of digital fundamental rights in EU history". Some have pointed to the "[undemocratic](#)" way it was rushed through without proper impact assessment or public consultation. Others noted the legal challenges that the proposal could face, including violating [proportionality](#), [procedural](#) and [fundamental rights](#) safeguards that underpin EU law. The European Ombudsman has already opened an [enquiry](#) into serious procedural flaws with the simplification proposal.

On the other hand, many proponents point to the complexity of the European digital rulebook. According to one [count](#), there are over 117 regulations that affect the digital sphere, with massive overlaps and fragmented implementation creating legal uncertainty for businesses. There is no doubt that businesses of all sizes face byzantine regulatory requirements that increase the cost of doing business. This is also hurting investments – according to Eurostat [data](#), gross fixed capital formation in the EU contracted by 1.9% in 2024. A recent BusinessEurope economic [survey](#) pointed out that almost half of all its EU members (industry and services companies) feel that the overall business climate in their countries has worsened from six months ago. However, this is clearly not down to regulation alone.

The 'simplification' agenda is born out of a fear that Europe has excessively regulated its technology sector. This fear is driven by chronic underperformance: in the last two decades, instead of driving a share of the world's technological advances proportionate to its economy, the EU finds itself falling behind the US and China as its economy shrinks. Both its startups and traditional industries are dependent on powerful foreign companies for basic digital infrastructure.

A host of reasons explain why Europe is lagging behind, but few would disagree that [fragmentation is perhaps the central cause](#). This includes the lack of serious VC and patient capital, 27 different VAT regimes, legal and compliance uncertainties and much more – highlighted in the [Letta report](#). The European Commission recognises this, which is why, in addition to simplification, the [EU Competitiveness Compass](#) highlighted new initiatives. These include the [28th regime](#) that aims to put in place EU-wide incorporation for startups, and the [Savings and Investments Union](#) – the latest attempt to find a way towards [completing the Capital Markets Union](#) after repeated failures.

The death knell of the 'Brussels effect'?

These changes have already been classified as the [death knell of the 'Brussels effect'](#), a term coined by Professor Anu Bradford in 2012. Brussels' regulatory approach was considered the gold standard in digital, and notably in the area of data protection. Multinationals found it easier to simply implement GDPR across jurisdictions, and a growing number of countries across the world implemented GDPR-inspired regulations, from India to Mauritius, and from Japan to Brazil.

Yet, if the cuts are as broad and deep as civil society has assessed, what should other countries think as they purportedly implement their own versions of the EU's pioneering ideas on privacy, data, competition and AI regulation? Indeed, some countries, like [Kenya](#), are working hard to achieve a data adequacy ruling from the EU. The EU's own efforts to simplify may call into question whether it was worth the effort.

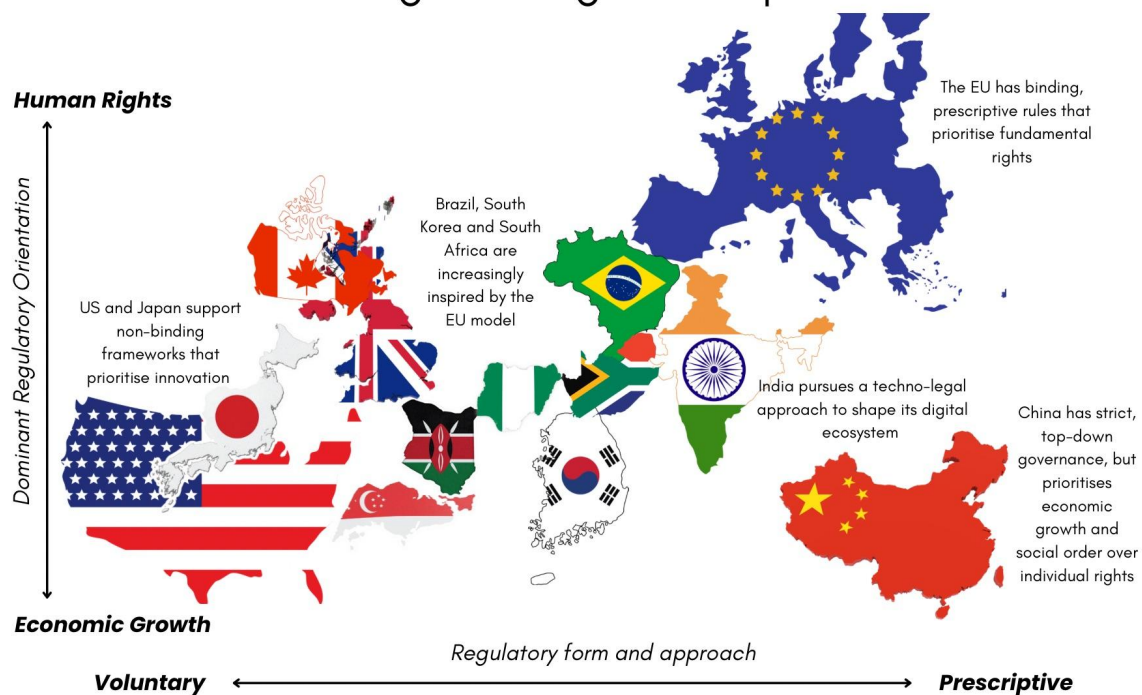
On the other hand, long before the digital omnibus, there was a growing questioning of the 'Brussels effect' across the world, with a number of countries contemplating a ['third way'](#) on digital regulations, to patch up the perceived inadequacies of the European approach. Critics around the world have pointed to the [unidirectional nature of the 'Brussels effect'](#), the lack of agency of those countries that were simply subject to the 'effect', and the lack of suitability to local contexts. Others highlighted the need for a more efficient means to reach an

agreement around data sharing and cross-border data flows. This was most notably highlighted by the Japanese with their work on '[data free flow with trust](#)', beginning with the G20 OSAKA Summit in 2019.

In some cases, flaws in the design and robustness of EU regulations themselves have revealed important lessons. To give an example, the [Digital Markets Act \(DMA\)](#), a landmark ex-ante regulation on ensuring fair competition in digital markets, failed to include cloud service and AI providers in its definition of 'gatekeepers' due to inadequacies in quantitative criteria. It now has to rely on qualitative criteria and has recently announced its intention to investigate the case for the designation of cloud hyperscalers.

This lesson was learned in Brazil. Following initial enthusiasm for regulating the market power of Big Tech with DMA-style regulatory tools, Bill 2768/2022 contained wide designation criteria and new regulatory powers for ANATEL (Brazil's telecom regulator). Yet, this bill was scrapped following [widespread criticism](#). Eventually, inspired by Germany, Japan and the UK, Brazil decided, instead of an ex-ante law, to create ex-ante rules, notified as [Bill No. 4675/2025](#), which directly amended Brazil's Competition Law (Law No. 12,529 of 30 November 2011) and granted new powers for Brazil's competition enforcer, CADE, instead of the telecom regulator.

How does the EU regulate digital compared to others?



Source: Authors analysis

ecdpm

India has been working on introducing a GDPR style privacy law since 2017 and has also learned from GDPR's shortcomings. In 2023, the Indian Parliament passed the [Digital Personal Data Protection Act](#) (DPDP Act), and two years later, the government started [implementing](#) the DPDP Act. The most notable difference between the GDPR and the DPDP is the notion of consent. The Indian DPDP does not recognise data processing without consent on any grounds (including "legitimate interests", a GDPR specific concept) and instead introduces a uniquely techno-legal approach called the [Data Empowerment and Protection Architecture](#) (DEPA), which contains technical protocols for a 'consent manager'. The Indian DPDP also requires AI developers (or all 'Data Fiduciaries') to obtain free, specific, and informed consent for each specified purpose, and to present notices that clearly itemise the personal data collected and the exact purpose behind its use. This means companies building AI training datasets must explain why they are collecting each data field, how they plan to process it, and how users can withdraw consent. Small exemptions on areas like research and publicly posted personal information add a bit of flexibility for AI companies. In general, this is a much more consent-preserving approach, which leverages technological solutions like the DEPA for enforcement.

While India may have considered the GDPR too lenient on consent, other countries looked for practical workarounds. As mentioned above, the Japanese pioneered the idea of "data free flow with trust", which was designed to function as a practical model for [achieving data adequacy with the EU](#), and for wider cooperation around cross-border data flows. The Japanese approach to regulating AI is also markedly different to the EU. Japan, as a key tech innovator, was early to consider AI governance, with systematic efforts dating back to December 2015, with its [Society 5.0](#) plan and vision. This was followed by the [Social Principles of Human-Centric AI](#) in March 2019, while in the interim (and up to 2022), several ministries issued non-binding guidelines for AI use, development, and governance. This 'principles-based approach' was followed up by the [Japan AI Act](#), which came into effect in September 2025, after the Japanese spearheaded the G7's Hiroshima Process, which was also non-binding. In the Japanese government's [own words](#): "Japan's approach to mitigating AI risks is to avoid excessive regulation", and this type of agile, multistakeholder, principles-based approach stands in stark contrast with the European approach.

Embedding regulation in code

What implications does this have for the reputation of the European Union as a bloc to emulate when it comes to digital regulation? Europe has historically played a key role in organising critical standards-setting bodies (CEN-CENELEC,

ETSI, 3GPP, etc.), which are driven by leading industry participants from across the world. The 'Brussels effect' exists not just due to the penchant of the European Union to write digital laws, but because companies from around the world have accepted these rules and work on implementing them through harmonised standards, i.e. the inclusive and open process of embedding regulation into code. If the EU is rushing through simplification of existing *acquis* – like the GDPR – while postponing large chunks of new landmark laws, like the AI Act, will this not cause uncertainty to industry and hamper its reputation as the world's pioneering tech regulator? What should partners, like Brazil, Kenya or India, think as they implement their own privacy and competition regimes?

There is a ray of hope for the 'Brussels effect' to hold. In our [interview](#) with leading Indian technology policy lawyer Rahul Matthan, he argued rather presciently that Brussels needs to embrace 'techno-legal regulation', i.e. work collaboratively with technologists to define protocols along with standards that maintain public interest and fairness in digital markets. A prime example of this is India's own experience with its digital identity – Aadhar – which has now permeated the daily lives of over a billion Indians – enabling authentication for both public and private tasks like grocery shopping, ride hailing, payments, financial services, personal loans, public service delivery, tax filings and much more. This digital identity layer powers the other parts of what is collectively called 'the India Stack' – India's population-scale digital public infrastructure, which is now [inspiring countries across the world](#).

Many EU countries have already introduced digital IDs, while almost all are in the process of doing so as part of the rollout of the [EU Digital Identity \(EUDI\) Wallet](#) regulation. This update to the eIDAS regulation mandates that all member states must introduce a digital ID as the first step towards a pan-European digital wallet, allowing access to public and private services across the EU, whilst maintaining high standards of privacy. Yet, some member states are also pioneers in digital public infrastructure like digital ID and secure data sharing, albeit at a smaller scale than India. [Estonia's eID](#), which complements [X-Road, its interoperable data sharing platform](#), is over twenty years old and is used by 99 per cent of its citizens. [Denmark's MitID app](#), introduced in 2021, is today used by more than 90 per cent of the population. [Spain's DNI](#) was introduced in 2006 and has since been complemented by the [MiDNI app](#), in a similar model to Denmark's. However, the introduction of the EUDI Wallet is set to be the major game-changer, building on interoperable national digital IDs in order to attain an EU-wide digital ID. It is due to come into force at the end of 2026. Recently, the European Commission also announced plans for an [EU Business Wallet](#), which mirrors the EUDI wallets for citizens.

The 'Brussels effect' is only relevant in a world where Europe is a significant single market, and EU rules are a relevant and effective benchmark for countries looking to establish legal frameworks that govern technology. The time has come for the Commission to scale this approach to build open protocols that help with the rollout of its regulatory framework. The EUDI wallet is the opening salvo by the EU to adopt a techno-legal approach and [keep the 'Brussels effect' relevant](#). Moving forward, this approach could facilitate the creation of cloud switching application programming interfaces (APIs), protocols for distributed social networks and much more.

Yet, there is no reason why Europe should do it alone. Moving forward, it must work with others like India, Brazil and Japan towards evolving the 'Brussels effect' into a '[Third Way](#)', much as Secretary S. Krishnan of India articulated at ECDPM when he was in Brussels last month. As Professor Lawrence Lessig has famously pointed out: "we can build, or architect, or code cyberspace to protect values that we believe are fundamental. Or we can build, or architect, or code cyberspace to allow those values to disappear. There is no middle ground. There is no choice that does not include some kind of building".

Acknowledgements

The authors would like to thank Melody Musoni for her peer review and Joyce Olders for support in formatting. The views expressed in this note are those of the authors and do not represent those of ECDPM or any other institution. Any errors or omissions remain the responsibility of the authors. For comments and feedback, please contact gk@ecdpm.org or cte@ecdpm.org.

References

AI Champions (N.d.). [EU Champions AI Initiative – Unlock Europe's Full Potential in AI](#). (Accessed 30 November 2025).

Alemanno, A. (2025). [The Omnibus Road to Constitutional Drift](#). Verfassungsblog.

Bradford, A. (2024). [The false choice between digital regulation and innovation](#). Chicago: Promarket.

Scott Marcus, J., Sekut, K. and Zenner, K (2024). [A dataset on EU legislation for the digital world](#). Brussels: Bruegel.

BusinessEurope. [BusinessEurope Spring Economic Outlook](#).

CADE (2011). [Law No. 12,529 of 30 November 2011](#). Conselho Administrativo de Defesa Econômica.

Câmara dos Deputados (2025). [Ficha de Tramitação: Bill No. 4675/2025](#).

Digital Agency, Japan (2024). [Data Free Flow with Trust \(DFFT\)](#). (Accessed 30 November 2025).

EDRI (2025). [Commission's Digital Omnibus is a major rollback of EU digital protections](#). (Accessed 30 November 2025).

EC (N.d.a.). [EU Data Union Strategy](#). Brussels: European Commission.

EC (N.d.b.). [The Digital Markets Act](#). Brussels: European Commission.

EC (2024). [EU-Japan deal on data flows enters into force](#). Trade and Economic Security. Brussels: European Commission.

EC (2025a). [Digital Omnibus Regulation Proposal](#). Brussels: European Commission.

EC (2025b). [Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. A Competitiveness Compass for the EU](#). Brussels: European Commission.

EC (2025c). [How “Once-Only” is at the heart of a ‘28th Regime’ in the EU](#). Brussels: European Commission.

EC (2025d). [Savings and investments union](#). Brussels: European Commission.

EC (2025e). [Joint Communication International Digital Strategy EU](#). Brussels: European Commission.

EC (2025f). [European Economic Forecast – Spring 2025](#). Institutional paper 318. Brussels: European Commission.

EC (2025g). [European Digital Identity \(EUDI\) Regulation](#). Brussels: European Commission.

EC (2025h). [European Business Wallets](#). Brussels: European Commission.

E-Estonia (n.d.). [X-road – Interoperability services](#).

European Ombudsman (2025). [Ombudswoman opens inquiry concerning how the Commission prepared a legislative proposal as part of its omnibus package of simplification measures](#). (Accessed 30 November 2025).

Eurostack Initiative (2025). [EuroStack – A European Alternative for Digital Sovereignty](#).

Fleming, S., Hall, B. and Foy, H. (2025). [Who killed Europe's single market dream?](#) Financial Times. (Accessed 1 December 2025).

German Federal Ministry for Digital and Transport (2025). [Summit on European Digital Sovereignty – Shaping Europe's digital future. Together](#).

Gobierno de España (n.d.). [Portal MiDNI](#)

Government of India (2023). [The Digital Personal Data Protection Act, 2023](#).

Government of India. (2025) [Digital Personal Data Protection Rules 2025](#). Ministry of Electronics and Information Technology (MeitY).

Government of Japan (N.d.). [Society 5.0](#). Cabinet Office.

Government of Japan (2019). [Social Principles of Human-Centric AI](#).

Government of Japan (2025). [Enjoying Japan's markets](#). (Accessed 30 November 2025).

Government of Spain (N.d.). [National electronic identity document](#). (Accessed 30 November 2025).

Haeck, P. and O'Regan, E. (2025). [Brussels is done being the world's digital policeman](#). Politico. (Accessed 27 November 2025).

Kirkwood, M. (2025). [Stopping the Brussels Effect: Big Tech and Brazil's Digital Markets Bill](#). Tech Policy Press. (Accessed 30 November 2025).

Krishnan, S. [Emergence of AI: Challenges & Opportunities for Europe and India](#). YouTube. Maastricht: ECDPM.

Letta, E. (2024). [Much More than a Market](#). Brussels: European Commission.

Lindner, J. (2024). [Capital Markets Union: Europe must stop beating around the bush](#). Hertie School Jacques Delors Centre.

Mariniello, M. (2025). [The European Commission's Digital Omnibus could increase risks, not growth](#). Brussels: Bruegel.

MitID (n.d.) [About MitID](#).

Newman, M. (2025). [Kenya nears EU data protection 'adequacy' decision, official says](#). MLex. (Accessed 30 November 2025).

NITI Aayog (2020). [Data Empowerment and Protection Architecture: A Secure Consent-Based Framework](#).

Noyb – European Center for Digital Rights (2025). [The EU Must Uphold Hard-Won Protections for Digital Human Rights](#).

Republic of Estonia (n.d.). [Electronic Identity eID](#).

Sambuli, N. (2025). [Glocalizing tech regulation](#). Development Ekko. (Accessed 30 November 2025).

Schoemaker, E. (2024). [Digital public infrastructure for sovereignty: What a "European" approach to DPI might look like](#). Global Policy.

Teevan, C., Kamath, G. and Hunter, J. (2025). [How India Stack could revolutionise EU tech policy](#). Maastricht: ECDPM.

Teevan, C. and Pouyé, R. (2024). [Tech sovereignty and a new EU foreign economic policy](#). Maastricht: ECDPM.