PAUL NEMITZ

EU digital policy in 2025: From the loss of orientation to reclaiming European leadership in the age of AI

Through landmark regulations like the General Data Protection Regulation (GDPR), the Digital Services Act (DSA), the Digital Markets Act (DMA) and the Artificial Intelligence (AI) Act, and an industrial policy aimed at digital sovereignty through broadening competences and supply of digital resources, the EU has positioned itself as the only continent with an innovative civilisational choice for the primacy of democracy and the rule of law over technology and business models. The year 2025 was to be the moment of consolidation for this genuine European vision of democratic and decentralised digital sovereignty, structurally embedded in EU digital regulation and policy.

Through landmark regulations like the General Data Protection Regulation (GDPR), the Digital Services Act (DSA), the Digital Markets Act (DMA) and the Artificial Intelligence (AI) Act, and an industrial policy aimed at digital sovereignty through broadening competences and supply of digital resources, the EU has positioned itself as the only continent with an innovative civilisational choice for the primacy of democracy and the rule of law over technology and business models. The year 2025 was to be the moment of consolidation for this genuine European vision of democratic and decentralised digital sovereignty, structurally embedded in EU digital regulation and policy.

However, a critical assessment of key developments in 2025 reveals not a coherent strategy, but a landscape riddled with profound contradictions and a growing crisis of credibility. These contradictions are symptoms of a deeper loss of strategic orientation and leadership, threatening to hollow out the EU's ambitious digital rulebook from within, and

thus, undermining democratic achievements and the good functioning of the rule of law, which are essential to a free and innovative society and economy.

The new potential for a majority coalition of centre-right and right-wing extremists in the European Parliament and the return of Donald Trump to the US presidency in late 2024 serve as a brutal catalyst for a new *Zerstörungslust*, a passion for destruction, as the sociologists Carolin Amlinger and Oliver Nachtwey write in their 2025 book with the same title.[1] The symptoms of this *Zerstörungslust* in the US are the application of Elon Musk's chainsaw to the US government; the claim that democratic laws and the United Nations are the 'antichrist' by Peter Thiel, the founder of PayPal and Palantir; and the National Security Strategy of US President Trump, which clearly aims to destroy democracy in Europe by announcing support for right-wing autocratic, populist parties in Europe.

This geopolitical shock coincides with internal moves in the EU, such as the European Commission's Omnibus 'simplification' package, ostensibly aimed at boosting competitiveness by reducing regulatory burdens. However, as applied to digital policy, this risks becoming a deregulatory gambit that weakens the very protections the EU has claimed to champion so far, without, however, providing an impetus for innovation or competitiveness in the common EU market.

Simultaneously, the operational choices of some member states and the European Commission betray its principles. Several European police forces are rapidly expanding their use of Palantir's 'Gotham' software – a predictive policing tool developed by the US company Palantir with deep ties to American intelligence and political figures like Peter Thiel, who aim to undermine democracy in Europe. There is no empirical evidence that crime has been reduced by this software, and many US police forces are already abandoning its use.

The European Commission failed to lead by example. In 2025, rather than using the decision of the European Data Protection Supervisor in 2024, demonstrating illicit data transfers and insufficient control over processing purposes in Microsoft 365 software, as a wakeup call to replace Microsoft with open-source software, as the German state of Schleswig-Holstein and the International Court of Justice are now doing, the European Commission continued the large-scale use of Microsoft. In 2024, it also signed new contracts worth hundreds of millions of euros with Amazon Web Services, thus not increasing digital sovereignty but rather digital dependence on US service providers, although cloud services have now become a commodity readily and reliably available in Europe according to state of the art standards, including AI services.

These contradictions cannot be viewed in isolation. They unfold against the backdrop of a new US global security strategy, which, under the current administration, explicitly frames geopolitics as a zero-sum contest of national interests, sidelining multilateral, rule-based frameworks. This strategy inherently seeks to undermine the aim of a cohesive and democratic EU and promotes a world order where power politics trumps the rule of law. In this context, the EU's internal vacillation and dependency are not merely self-inflicted wounds but strategic vulnerabilities. A coherent, assertive European leadership in digital

1 Amlinger, C. and O. Nachtwey (2025) *Zerstörungslust* (Berlin: Suhrkamp).

policy is no longer just an economic or regulatory preference; it is a geopolitical imperative for the survival of democracy and fundamental rights in Europe. This leadership must be rooted in the recognition, as articulated by Apple CEO Jim Cook at the global data protection summit in 2018 in Brussels, that in the age of pervasive, hyper-personalised AI, stronger data protection and privacy are not obstacles but prerequisites. Only with these robust guarantees can citizens trust the digital ecosystem, and only with trust can democracy flourish.

Therefore, 2025 underscores a pressing need: the EU must move beyond writing exemplary rulebooks and confront the hard task of rigorous, consistent enforcement and technological self-reliance. It must clearly counter a US tendency to bypass legal frameworks with power politics, a concept fundamentally at odds with the European project and a rule-based, peaceful global coexistence. The path forward demands closing the gap between rhetoric and reality, ensuring that its practice of digital policy making and enforcing digital law, as well as its digital industrial policy, is built on the solid ground of integrity and principles of the EU Treaties and the Charter of Fundamental Rights, not the shifting sands of contradiction and opportunistic obedience to arbitrary asks from the US.

The Omnibus proposal and the retreat from rigour: Simplification versus dilution

The 2025 DMA and DSA decisions of the Commission concerning Meta, Apple and X could be seen as honest enforcement efforts, although the fines imposed (between €120 and €500 million) are too small to lead to real change in trillion dollar digital empires.

In contrast, the European Commission's Omnibus simplification package launched in November is a direct response to the Draghi report[2] and the new US administration. The report's stark finding that the EU relies on foreign countries for over 80% of digital products, services, infrastructure and intellectual property and its loud – but unsubstantiated – critique of EU digital legislation inspired a fast but insufficiently reflective response, catering to vague, general and decades-long repeated claims of overregulation by a small group of activists in Europe, and US wishes for deregulation.

According to Max Schrems of the privacy and data protection non-governmental organisation (NGO) None of Your Business (NOYB),[3] the Omnibus package can thus be seen as a reactive, almost panicked, move to ease pressure on European businesses, which, however, has been proposed without a thorough impact assessment and serious prior consultations. In fact, in a pre-implementation consultation round with the responsible Commissioner for Democracy, Justice, the Rule of Law and Consumer Protection, Michael McGrath from Ireland,[4] none of the proposals for changes in GDPR in the Omnibus

2 Draghi, M. (2024) "The future of European competitiveness". European Commission.
3 "Digital Omnibus: EU Commission wants to wreck core GDPR principles". NOYB, 19 November 2025.
4 Ibid.

package had been asked for by stakeholders, according to Max Schrems and NOYB, who participated in the consultation round.

NOYB identifies several fundamental threats to data protection in the Omnibus package. The proposal would narrow the definition of 'personal data' through new concepts, such as 'pseudonyms' or 'IDs', potentially exempting many companies from GDPR requirements altogether, at the expense of individuals. Critically, the reforms would introduce a 'legitimate interest' exception, allowing companies to use personal data, including some sensitive information, for AI training without explicit user consent. Schrems argues this gives tech giants a blank check to collect European data, noting that users would rarely know their data is being used and would find objections nearly impossible to enforce.

The proposal would significantly weaken protections for sensitive information, including health data, political views and sexual orientation. It would also enable remote access to personal data on devices without user consent. NOYB warns these changes conflict with the EU Charter of Fundamental Rights and established Court of Justice case law.

Despite claims that reforms would help small and medium enterprises, Schrems argues that the opposite is true. The changes primarily benefit large technology companies while creating legal uncertainty that will require expensive legal advice, ultimately increasing market concentration. He notes enforcement is already weak, with fewer than 1.3% of GDPR complaints resulting in fines, and these reforms would make successful enforcement even rarer.

NOYB emphasises that most EU member states explicitly asked not to reopen GDPR, and 127 civil society organisations, alongside major European Parliament groups (S&D, Renew and Greens), have criticised the Commission's approach. The reforms appear, according to NOYB, to be driven by external pressure, possibly from German government influence or American business interests, rather than democratic consensus or genuine evidence of need.

Also, as to GDPR, while the new procedural regulation, which was adopted by the Council in November, is noteworthy, more attention should be given to the fact that the European Commission did not suspend transfers of personal data to the US. The adequacy finding of the Commission with regard to the US relies in great part on the independence of the Federal Trade Commission (FTC) and the Privacy and Civil Liberties Oversight Board (PCLOB), both of which are the target of President Trump's drive to bring all independent authorities within the US governance system under his control. With the new aggressive anti-European National Security Strategy, the time has come for the Commission to suspend data flows, for the same reasons that the US considered data flows to China by Americans a national security problem and because the actions of the US administration with regard to the FTC and the PCLOB in particular clearly no longer provide the guarantees that formed the basis of the adequacy finding.

The key criticisms of the Commission's Omnibus proposal of November 2025, regarding the delayed entry into force of the EU AI Act and the interim codes of conduct adopted in 2025, revolve around two major concerns: the creation of a governance vacuum and the inadequacy of voluntary measures.

Firstly, the 2-3 year delay (pushing full enforcement to 2026-2027) has been widely condemned by consumer protection groups, digital rights NGOs and some member states as a dangerous and irresponsible pause in accountability. Critics argue that this delay grants high-risk and foundation model developers an unwarranted 'grace period' during a phase of explosive technological growth. This regulatory gap, they contend, leaves citizens exposed to potential harms – from biased hiring algorithms to opaque public surveillance systems – without legal recourse. The delay is seen as a major victory for industry lobbyists, prioritising corporate profits over public safety and fundamental rights. It also ignores that both the negotiation time and the time until entry into force have already left corporations enough time to prepare to comply with the AI Act and that there is thus really no justification for delaying the entry into force. In particular, the argument that in the absence of technical standards the law cannot be properly applied, makes the application of democratic law dependent on technical standards, the adoption of which is blocked by industry representatives, which is unacceptable.

Secondly, the 2025 voluntary codes of conduct, intended as a bridge to full regulation, are criticised as being toothless and insufficient. These codes, developed in multi-stakeholder forums but heavily influenced by major tech firms, lack independent monitoring, clear sanctions and meaningful enforcement. Without the binding obligations and hefty fines (up to 7% of global turnover) stipulated in the AI Act, critics argue they function as 'ethics washing', allowing companies to make vague commitments while continuing risky practices. Key elements of the AI Act, such as mandatory fundamental rights impact assessments, conformity assessment procedures and transparency requirements for general-purpose AI systems, are either absent or diluted in these non-binding pledges.

In summary, the criticism is that this combination of delay and weak voluntary codes fatally undermines the EU's proclaimed goal of being a global standard-setter for trustworthy AI. It creates a prolonged period of legal uncertainty where market dynamics, rather than democratic rules, set the pace. Critics warn this approach risks repeating the mistakes of the social media era, where delayed regulation allowed systemic harms to become entrenched before lawmakers could respond.

Reclaiming European leadership in the age of AI

The events of 2025 serve as a critical inflexion point. The EU stands at a crossroads between continuing as a fragmented 'regulatory state', increasingly ignored by global powers due to a lack of rigour in enforcing its laws, and transforming into a genuinely sovereign digital power. The contradictions embedded in the omnibus proposal, the Palantir contracts and the Commission's lack of leadership in terms of engagement with open-source and European service providers for its own operating needs are symptoms of a leadership vacuum. To reclaim its role, the EU's outlook for 2026 and beyond must be guided by a coherent, uncompromising strategy built on four pillars:

1) From simplification to strategic enforcement: the EU must abandon a deregulatory 'simplification' that weakens substance. Instead, it must invest massively in enforcement capacity. This means adequately funding the European Commission's DG COMP and DG CONNECT for DMA/DSA enforcement; empowering a unified and well-resourced AI Office; and fostering seamless cooperation between national data protection authorities, digital services coordinators and market surveillance bodies to reduce the costs of fragmentation. The goal must be to make non-compliance more costly than compliance, thereby giving real teeth and incentives to comply with EU law for the lawless players of Big Tech who have a well-known and long track record of lying and breaking the law.

2) From rhetorical sovereignty to technological sovereignty: the EU must match its regulatory ambition with industrial and financial commitment. Initiatives like AI factories; federated digital, data and AI infrastructure; and the proposed EuroStack for digital infrastructures must move from pilot projects to default options for public procurement. EU institutions and member state governments must use their collective purchasing power to create a guaranteed market for European alternatives in cloud services, cybersecurity, public service and public communication platforms, and AI services, consciously phasing out dependencies on firms like Palantir, Microsoft, Amazon Web Services, Google and Meta and systematically advantaging open-source and federated networks.

3) Leading by unassailable example: European institutions must become gold-standard exemplars of compliance and lead market buyers of digital and AI products serving European digital sovereignty. The Microsoft 365 decision of the European Data Protection Supervisor should trigger a full audit of all third-country software dependencies within the EU and member state governments. Procurement rules must mandate verifiable data sovereignty, open standards and interoperability, as well as key principles such as public code and public data for public money, democracy impact assessments and democracy by design in any programme or AI system implemented in public services. Digital policy must become a central part of the defence of democracy, as on the other side of the Atlantic, President Trump aims to use digital tech giants to undermine democracy. Just like Europe must learn to defend itself without US support and US weapons, it must learn to design and regulate its digital and AI environment without dependence on either US or Chinese tech companies.

4) Asserting a democratic counter-vision in the age of AI: in response to a US strategy that often sidelines multilateralism for power politics, the EU must confidently articulate and demonstrate that its model is superior. As Apple's Jim Cook noted, extreme AI personalisation requires extreme data protection – this is the EU's foundational insight. The EU must now prove that a world governed by the rule of law, democracy and fundamental rights is not only more ethical but also more innovative, stable and resilient. This means rigorously applying the EU Digital Law and the AI Act's risk-based framework, banning social scoring and manipulative practices, and ensuring that the 'human-centric' promise is more than a slogan. It also means that the adequacy finding with regard to the US must be revoked by the Commission and data flows to the US suspended, both because the US no longer provides guarantees for independent oversight through the FTC, PCLOB and

National Security Courts, but also because the US could use the personal data in its drive to undermine European democracy, in line with the new National Security Strategy.

The US administration's approach makes the need for a strong, sovereign and democratic Europe not a choice but a necessity. The EU's digital policy must become the bedrock of that sovereignty. By closing its credibility gap, enforcing its laws without fear or favour, and building its own technological base, the EU can transform from dependency and obedience to US pressures into a genuine global leader of tech for democracy. Only then can it ensure that the digital age, and particularly the age of AI, strengthens rather than undermines the democratic and common legal foundations upon which it was built.