Hertie School
Jacques Delors Centre

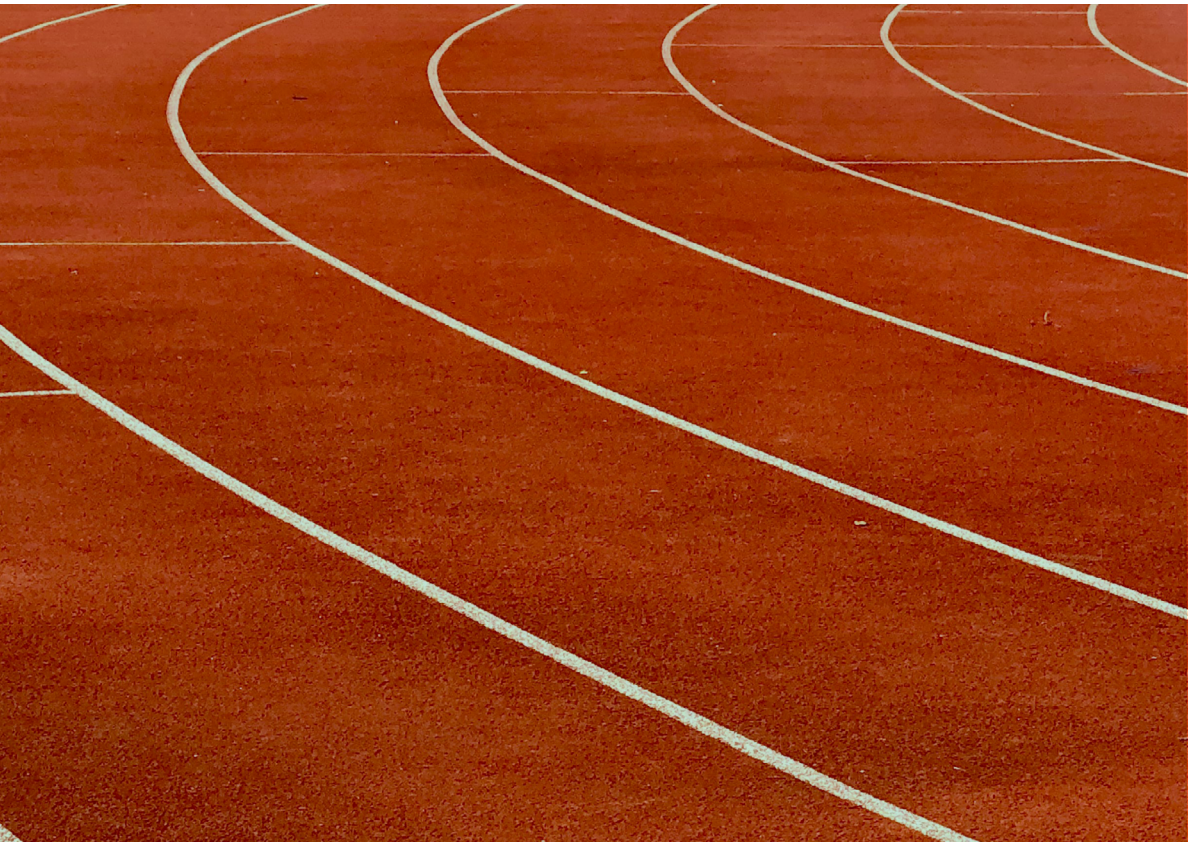
Vision for Europe

Beyond Dependency

Enforcing EU Rules Against US Big Tech

19 October 2026

Luise Quaritsch, Policy Fellow



Europe is overwhelmingly dependent on US Big Tech. The EU recognises the related costs and risks to its security, competitiveness and democratic self-determination and wants to build up European alternatives. But US Big Tech's market dominance has created structural advantages for the incumbents and high barriers to entry. The EU must give its regulatory power more muscle, especially in evolving digital markets, ensure substantive compliance and improve the enforcement structure of its digital rulebook.

Europe is overwhelmingly dependent on US Big Tech.[1] Apple, Microsoft, Google, Amazon and Meta[2] provide the EU with a large share of its digital infrastructure and services. The EU imports digital services worth more than €300 billion annually from the US. With their overwhelming market power, they shape how Europeans communicate, do business, consume information and engage in public discourse. The broad adoption of AI applications could further entrench this power.

This dependency comes with risks and costs for Europe's security, economy and democracy. Where US Big Tech provides European countries with essential digital infrastructure or handles sensitive data, for example for defense agencies, the US government could demand access to that data and hold a "kill switch" – the ability to cut off essential services. From an economic perspective, US Big Tech's dominant position in highly concentrated digital markets makes it difficult for new competitors to emerge, stifling innovation and limiting consumer choice, while its outsized market power allows it to drive up prices. In addition, Big Tech companies control what information is seen and can shape public discourse, with significant consequences for democratic processes. Their vast financial resources allow them to sustain extensive lobbying, far exceeding other industries, aimed at shaping EU legislation and regulatory oversight.

The EU has recognised these risks and is pursuing more digital sovereignty. The European Commission presented a Tech Sovereignty package on 3 June 2026, aimed at strengthening the EU's digital autonomy in key technologies such as Cloud and AI development. The goal here is to "boost indigenous innovation, homegrown industrial capacity and autonomy" along the digital technology supply chain. But without contestable digital markets,[3] it will be difficult for European companies to attract the massive investment necessary and then to compete. At the same time, the EU aims to regulate the conduct of Big Tech companies that provide quasi-public digital infrastructure in order to protect citizens' rights, data and democratic processes in the online space.

So far, that regulation has been only modestly successful. US companies are uniquely powerful enterprises and notoriously difficult to regulate. The EU has introduced a number of new regulatory tools in recent years such as the Digital Markets Act (DMA) and Digital Services Act (DSA), specifically aimed at very large online platforms and companies that act as gatekeepers, controlling access to technology for end users. European regulators have fined Google, Apple, Meta, Amazon and Microsoft more than €20 billion[4] since the start of 2021. Nevertheless, problematic business practices, high market concentration and dependency remain largely unchanged.

Difficulty enforcing the EU's digital rulebook are exacerbated by US Big Tech's alignment with the Trump administration. The US government has taken an aggressive stance towards the EU's digital rules and classified them as "non-tariff barriers" to trade and discriminatory to the US tech sector. US trade officials have threatened retaliatory measures should the EU continue to uphold its rules. This convergence of state and private power has enabled these private companies to rely on US foreign policy instruments

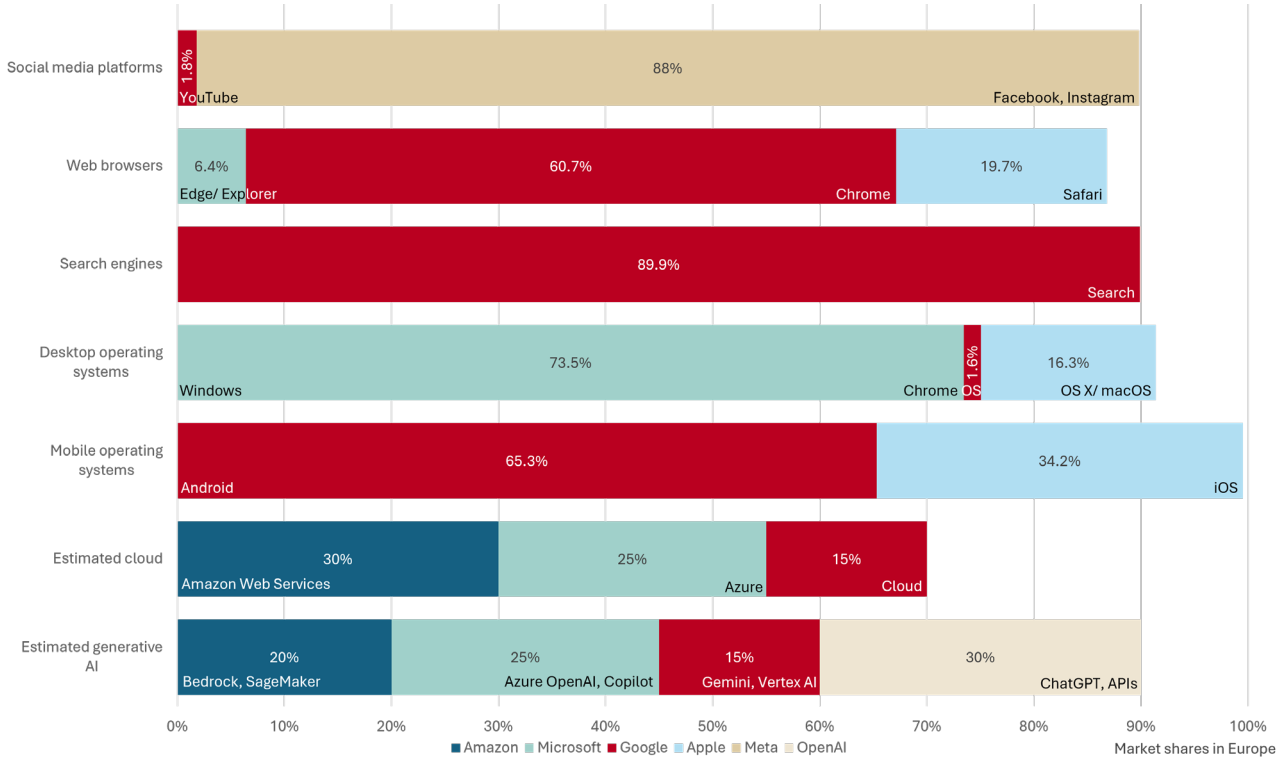
1 In preparation of this policy brief, the Jacques Delors Centre hosted an expert workshop in June. The author thanks all participants for their time and valuable insights. The views and opinions expressed in this brief are solely those of the author.
2 Often referred to collectively as GAMAM.
3 There are, of course, several other decisive factors here. See the Eurostack 2025 report for a comprehensive strategy for European digital sovereignty.
4 See table attached.

and coercive tactics to defend their interests, ostensibly with success. There have been numerous reports that the Commission has yielded to this pressure.

EU regulators need to find ways to rein in US Big Tech more effectively. The EU wants to become more digitally independent, strengthen its competitiveness on digital markets and protect democratic values and fundamental rights online. Effective regulation of US Big Tech is central to achieving those goals. This paper takes stock of US Big Tech's dominant position and lays out why this dependency is a risk for European security and democracy, harming European businesses, consumers and citizens. It analyses the limited impact of current EU regulation and proposes three areas in which the EU can make its regulatory interventions more effective: Addressing market power more rigorously to level the playing field, taking steps to substantively change US Big Tech behaviour, and tackling enforcement gaps.

US Big Tech's dominance across Europe's digital markets

The dominance of US companies across digital markets is striking. Europe's digital markets are highly concentrated, with a small number of powerful firms holding leading positions across core services and infrastructure: According to a study published by the European Parliament, Meta's Facebook and Instagram dominate the social media market. Google Search exceeds 89% of web searches and most Europeans use US providers' web browsers. Around 80% of EU corporate spending on software and cloud services flows to US vendors. Google's Android and Apple's iOS command virtually 100% of mobile operating systems. Microsoft's Windows holds a 73% share of desktop operating systems, while Apple's operating system accounts for most of the rest. Amazon, Microsoft and Google hold almost 70% of the European cloud market. Public administrations rely heavily on Microsoft and Google productivity suites and US cloud services.



Source: European Parliament Report "European Software and Cyber Dependencies"(2025) https://www.europarl.europa.eu/RegData/etudes/STUD/2025/778576/ECTI_STU(2025)778576_EN.pdf. Web browsers, social media platforms, search engines, mobile and desktop operating systems: StatCounter Global Stats (based on number of page views, as of the end of July 2025), Cloud: Synergy Research (2024). Own illustration.

Figure 1: US Big Tech dominance in EU digital markets.

This dominance can partially be explained by the fact that digital markets are prone to creating monopolies. Reinforcing network and lock-in effects are characteristic: The more users a platform has, the more it attracts. This creates tipping points and leads to one or two companies capturing most of a market. Once users are on a platform, they can be easily locked-in by practices that make switching to a different service costly. For example, leaving the dominant social media platform can mean losing data and access to a social or professional network. Contractual hurdles may also prevent people from switching. Economies of scale, meaning the ability of large tech firms to expand their user base at a decreasing marginal cost per user, have also benefited incumbents. US Big Tech companies have successfully leveraged these effects, as well as existing customer bases and anti-competitive practices such as bundling different tools, services and hardware, to become dominant across digital markets. One recent example is Microsoft's bundling of its collaboration tool Teams with its Office 365 productivity suite to leverage the latter's vast user base. Big Tech companies have created closed ecosystems with high switching costs, so the most convenient choice for users is one provider across all services and devices.

In addition, as data becomes an increasingly valuable economic resource, companies benefit from their large customer base. The more users a tech company has, the more data it can collect. That data can be monetised through advertising or selling it to other businesses. It can also be used to improve a product, creating a feedback loop that reinforces dominance. For example, Google has by far the most widely used search engine and can use the data from its users – such as what they click on or how many queries they make – to improve its results. This is a great advantage over any new competitor.

To keep a dominant position, Big Tech companies have also strategically acquired other companies. Big Tech companies have been able to consolidate their power and dominate innovation in their fields by strategically acquiring start-ups and potential competitors: Google bought Android in 2005 and YouTube in 2006, Microsoft bought LinkedIn in 2016, Facebook bought Instagram in 2012 and WhatsApp in 2014. Facebook's internal documents revealed that these acquisitions were intended to "neutralise potential threats". In this context, Facebook's CEO Mark Zuckerberg wrote in an e-mail that it was "better to buy than to compete". According to an NGO report, Google, Amazon, Apple, Meta and Microsoft bought at least 191 companies globally between 2019 and 2025. In 2025, unsurprisingly, AI-related acquisitions dominated Big Tech's expansion strategy.

The cost of dependency for Europe

Europe's dependency on US Big Tech has become a security risk. As geopolitical tensions intensify and the United States has become an increasingly unpredictable ally, the vulnerabilities created by this dependence are becoming more apparent. As Commission President Ursula von der Leyen stated on the release of the Tech Sovereignty package: "We cannot afford to depend on others for the technologies that keep our hospitals running, our energy grids stable and our services secure." A central concern is that relying on US providers for essential digital and physical infrastructure – like data centers or infrastructure used in sensitive areas for military operations – could hand a "kill switch", the ability to cut off access to digital services, to the American government. In 2025, the Trump administration imposed sanctions on prosecutors and judges of the International

Criminal Court (ICC) over their investigation of Israel. The measures prohibited US companies from providing services to sanctioned individuals and blocked the judges from using companies like Amazon, Airbnb, PayPal, Visa and MasterCard. If the US imposed such sanctions against European government officials, it could keep them from accessing their e-mails or travelling, for example.

In addition, US authorities can request far-reaching access to European data when it is stored by a US parent company. Under the CLOUD Act, US authorities can force American companies to share data stored in their cloud infrastructure, regardless of where the data is stored physically. Relying on US cloud infrastructure for sensitive information can turn into a serious security risk, as the Trump administration has proved increasingly willing to deploy aggressive measures against other countries. This is a particularly high risk in the defense field, where a majority of EU countries rely on US cloud providers for their defense agencies.

Concentrated digital markets limit European competitiveness and raise prices for European businesses and consumers

In addition to these obvious security risks, the EU's lack of competitiveness on digital markets also has costs. Big tech companies act as gatekeepers to digital infrastructure, providing app stores, search engines, and marketplaces to consumer, for example. As key intermediaries between businesses and consumers, they can design infrastructure that favors their own services, extract gatekeeper rent from other businesses and leverage their position to expand into other markets. For European companies that want to compete with the services Big Tech offers, this tilts the playing field. These high barriers make it difficult for European businesses, even if they are more innovative or efficient, to challenge the incumbents that profit from their closed ecosystems. For example, Amazon and Google not only provide digital infrastructure like a marketplace or search function, they also compete on those markets and can give their own products preferential treatment. Google has been found to have favored its own services such as shopping, hotels or transportation, in search rankings, disadvantaging European alternatives. Amazon has reportedly used its marketplace data to copy other sellers' goods and then manipulated search results to favor its own products.

For business users, market concentration comes at a cost as well. Dominant platforms can leverage their market power to impose unfair or even exploitative terms on business users. With no comparable alternatives, business users often have no choice but to accept them. For example, app developers rely on the App Store to distribute their products on Apple devices. Apple used that position to force developers to use its own in-app purchase system and charged a 30% commission on all subscription fees. It did not allow developers to inform users of alternative, potentially cheaper, purchasing possibilities. In the advertising market, Google and Facebook are dominant. According to a report by the UK's Competition and Markets Authority, this has enabled Google to demand significantly higher prices than competitors (30-40% higher for search advertising) and Facebook to generate much higher revenue per user than other social media platforms. In the cloud market, some studies indicate that European providers charge significantly less than the dominant American companies. While it may not be possible to quantify these mark-ups across the entire economy, their cumulative cost is likely to be substantial.

For consumers, Big Tech dominance means limited choice and less control over their data. Like businesses, consumers often have to rely on Big Tech platforms and accept their terms and conditions, as there are no real alternatives. With business models based on advertising and companies profiting from collecting as much data as possible, consumers are likely sharing more data with platforms than they would like to. In addition, platforms often design their processes to make it difficult for consumers to choose anything but the default settings. Where companies collect data from one service, they can often use that data to strengthen another part of their business. Big Tech companies' business practices have also often raised fundamental rights concerns over their data collection and user profiling.

US Big Tech's power is a challenge to European democracy

The power of US Big Tech companies also risks undermining the EU's democratic principles. Their revenues often exceed that of states. The overwhelming economic power they have amassed, increasingly in convergence with US state power, means they can evade regulations that apply to other market actors. This undermines democratic institutions' ability to exercise oversight over these companies. It is also a challenge to Europe's democratic self-determination when foreign companies and governments exert pressure to change how economic activity is regulated in the EU. This is particularly concerning given that many US Big Tech companies control not just markets but also information and communication services. They act as providers of quasi-public infrastructure – and their leadership is not without political agenda. Elon Musk's takeover and restructuring of Twitter is a clear example of that. These companies' design choices, which shape the information environment, largely escape public control – despite public interest.

The discursive power that Big Tech companies hold in increasingly digital societies is significant. By organising search results, curating and moderating social media feeds, designing recommender algorithms and programming AI systems, US Big Tech companies are not just neutral facilitators of access to information. They have monopoly power to shape what information is seen. Those design choices on social media have had discernable effects on political debates. With extreme voices amplified, social media platforms have been shown to have a polarising effect on public debate. They have also acted as gateways for malign foreign information manipulation campaigns. Media outlets meanwhile struggle to maintain their independence in an information environment where Big Tech companies control visibility and monetisation by guiding web traffic.

Generative AI is exacerbating these issues. Generative AI can increase the profitability of individualised digital ads by lowering the costs to create them. It can also produce political content that is used to trigger outrage at very low costs. Moreover, AI overviews and Chatbots extract and present information from news sources without remuneration mechanisms for the publishers. This diverts traffic from news publishers, threatening their business models. In addition, the sources of AI-generated content are often opaque and potentially vulnerable to manipulation by malign actors, such as spreading Russian disinformation. Malign actors churn out websites and content specifically to influence the results of AI chatbots while reputable sources of information increasingly protect their sites from AI crawlers, depreciating the quality of information AI chatbots rely on. The intransparent nature of the information generated by AI chatbots in private conversations, generally trusted by users, puts even more control over the information ecosystem in the hands of Big Tech.

There are several ways in which regulation can tackle the power of large firms, and the associated risks and costs outlined above. First, it can challenge companies' market dominance and economic power, with the aim of making digital markets more competitive and reducing structural dependence on a small number of firms. Second, it can regulate their conduct and business practices in areas where they act as gatekeepers or provide quasi-public digital infrastructure. These are distinct but mutually reinforcing objectives: the first seeks to change the structure of the market, while the second seeks to constrain the exercise of power where dominant platforms remain essential intermediaries. Both can ultimately reduce the dependency on US Big Tech or the risks of that dependency.

The EU's initial approach to rein in the tech market through competition law failed. Competition law, the EU's traditional instrument to protect competition and prevent abuse by market dominance, proved ill-equipped to tackle the new challenges that the fast-paced digital transformation and emerging tech giants have presented. The focus of competition policy on short-term consumer welfare, measured in prices, cannot capture power concentration in the digital economy where users are not necessarily charged for a service and data is a valuable asset. In the 2000s and 2010s, this allowed tech companies to accumulate power while largely evading regulatory scrutiny, both in the US and in the EU. In the area of merger control, for example, the European Commission did not review Facebook's 2012 acquisition of Instagram because Instagram's turnover was below the notification threshold for mergers – even though Facebook paid $1 billion for the photo-sharing app. When Facebook bought WhatsApp in 2014, the European Commission found that the merger did not raise competition concerns. Privacy concerns over the potential combination of Facebook and WhatsApp user data did not feature in the investigation. Overall, case-by-case antitrust enforcement against abuses of dominance proved to be too slow and insufficient for fast-moving markets prone to concentration and with structural competition problems.

Other negative effects of Big Tech's conduct and business models were also not fully captured by existing legislative frameworks. More and more evidence of the risks and harmful consequences associated with Big Tech, in particular of social media platforms, has surfaced in recent years: the amplification of disinformation and illegal content, the distortion of democratic debate and its impact on elections, negative effects on public health, data protection and the well-being and safety of children online. The EU's earlier digital rulebook was not designed to address these systemic risks. The 2000 e-Commerce Directive primarily limited intermediary liability instead of addressing the design of recommender systems, content moderation and how platforms should deal with illegal content.

As a reaction to these new challenges, the EU has introduced a number of laws in recent years. Most notably, from a competition perspective, the Digital Markets Act (DMA) aims to support fair digital markets by introducing pro-competitive obligations on digital platforms with gatekeeper positions.[5] It creates *ex-ante* rules for gatekeepers to complement ex-post competition enforcement. By setting these rules, the DMA also aims to make digital markets more contestable and more competitive to promote innovation and consumer choice. This includes the obligation to inform the Commission about any relevant merger. Other recent regulation of digital markets includes the Digital Services

5 Currently Alphabet (Google), Amazon, Apple, Booking, ByteDance (TikTok), Meta and Microsoft.

Act (DSA). It sets obligations for "very large online platforms and search engines"[6] with over 45 million monthly EU users to make the online environment safer for citizens and consumers. Those large platforms now have to identify and mitigate any "systemic risks" that arise from their services. Both the DMA and the DSA have been applicable in the EU since February 2024. Even more recently, in August 2026, the EU's AI Act has entered into force. Taking a product safety approach, it aims to improve the transparency of AI systems and introduces risk-mitigation requirements for high-risk AI. The EU's main data protection law, the General Data Protection Regulation (GDPR) has been in force since 2018. It regulates how tech companies collect, process and monetize users' personal data, limiting their ability to exploit data-driven market power.

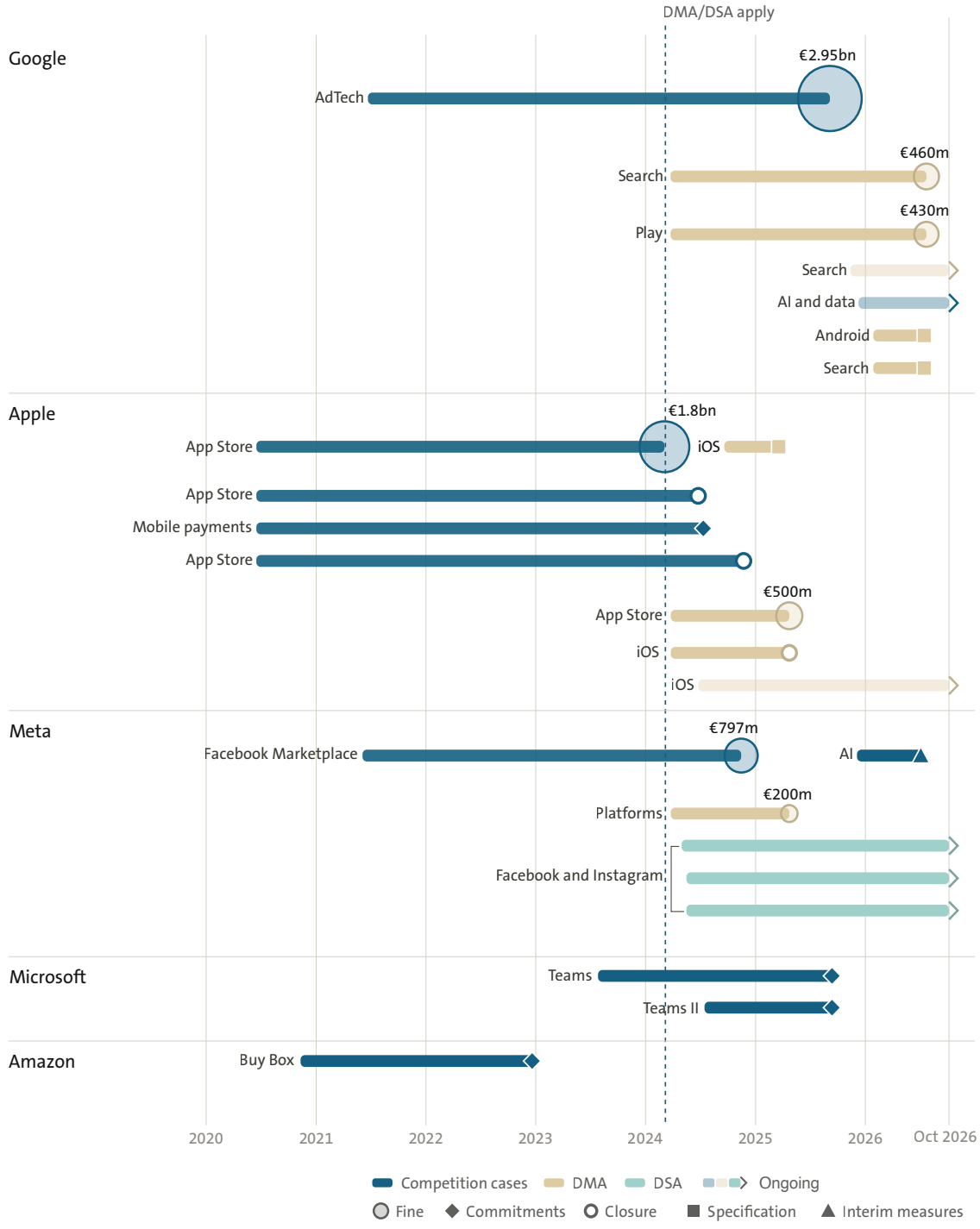


Figure 2: Overview of the EU's recent enforcement action against US Big Tech.

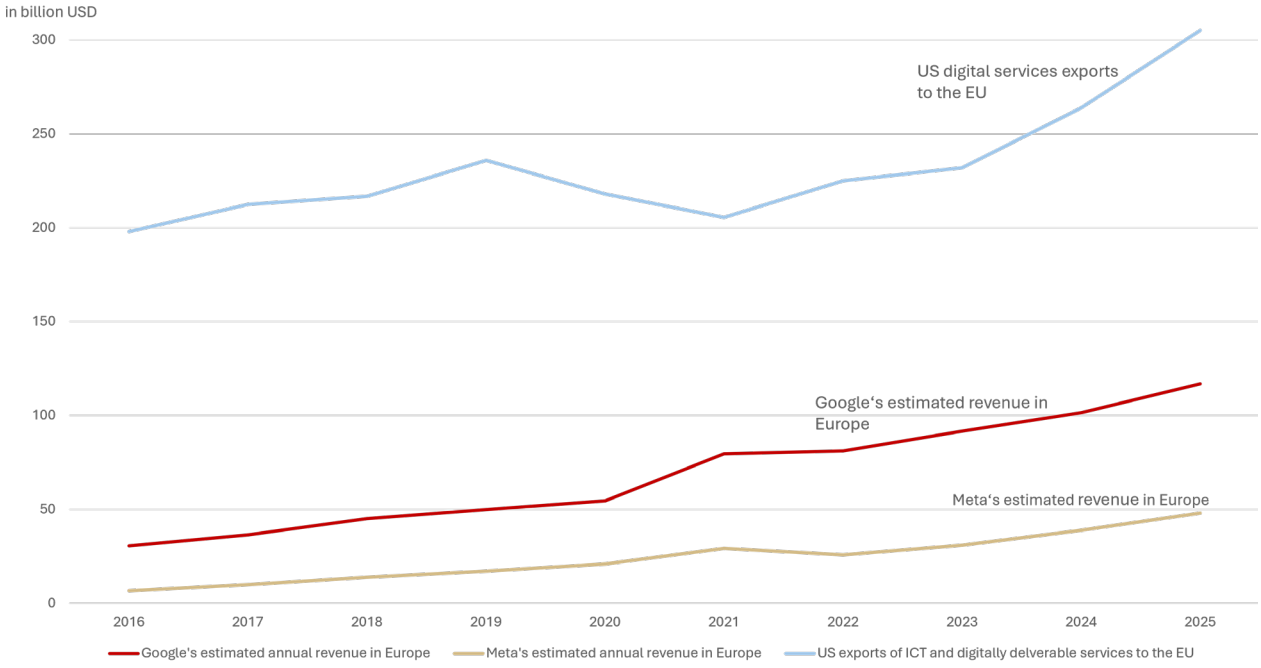
6 Designated VLOPs/VLOSEs by GAMAM providers: Amazon Store; Apple App Store; Google's Search, Play store, Maps, Shopping, and YouTube; Microsoft's LinkedIn and Bing; Meta's Facebook and Instagram.

These laws are currently being enforced against all major US Big Tech companies. The Commission has started seven compliance investigations under the DMA. Four non-compliance decisions have been issued so far: Two against Google and one decision against Apple and Meta respectively. All four decisions included fines, totaling €1.59 billion, and an obligation to stop the breach. One investigation against Google and one against Apple are still ongoing, another one against Apple has been closed because Apple changed the policy concerned. Under the DSA enforcement framework, the Commission has requested information from all US Big Tech providers of online platforms to verify their compliance.[7] It has opened proceedings against Meta for suspected breaches of at least 14 different obligations and published preliminary findings in three cases for both Instagram and Facebook. The Commission has also opened 12 competition law cases against US Big Tech since 2020 and issued fines amounting to €5.5 billion. National data protection authorities, in charge of enforcing the GDPR, have fined US Big Tech companies more than €3 billion. Eight out of 11 cases are fines against Meta services by the Irish Data Protection Authority. Overall, US Big Tech has been fined more than €20 billion in the last six years (see table attached for an enforcement overview).

The limited effects of regulatory interventions to date

Overall, the EU's new digital rules have not challenged US Big Tech's market power. They have neither meaningfully curbed the market dominance of US Big Tech companies nor their harmful business practices. Concerning market structures, both the DMA and competition law have been enforced against Big Tech companies and placed obligations on their conduct, with the underlying goal of making digital markets more contestable. But it is difficult to measure whether they have achieved these goals due to limited market data and because establishing causality between new legal obligations and an altered market structure is difficult. Nevertheless, the indicators currently available do not point to a changing market. Except for Facebook Marketplace, no gatekeeper has lost substantial market share, nor their status, since having to comply with the DMA obligations. US Big Tech firms' revenue in Europe continues to grow and the EU's import of digital services from the US has risen sharply from around €200 billion in 2016 to more than €300 billion in 2025. Globally, market concentration has continued as well. The top five digital enterprises have increased their share of sales from 21% in 2017 to 48% in 2025.

7 Has requested information from Google (e.g. YouTube), Microsoft (LinkedIn), Amazon (Store), Apple (App Store).



Source: US export:Bureau of Economic Analysis, US Deportment of Commerce (2026) Table 3.3. U.S. Trade in ICT Services and Digitally Deliverable Services, by Country or Affili https://www.bea.gov/?_gl=1*14ilz6p*_ga*MTcyMjY0NTM0LjE3OTE4OTQ5MzY.*_ga_J4698JNNFT*czE3OTE4OTQ5MzYkbzEkZzAkdDE3OTE4OTQ5MzYkajYwJGwwJGgw. Meta: Statista (https://www.statista.com/statistics/745351/facebooks-quarterly-revenue-in-europe/. Google: Statista (2026) https://www.statista.com/statistics/266250/regional-distribution-of-googles-revenue/ https://www.statista.com/statistics/266206/googles-annual-global-revenue/

Figure 3: Google's and Meta's estimated annual revenue in Europe and the US exports in digital services to the EU

At most, the DMA has made digital markets formally more contestable. The Commission's first review of the DMA this year highlights that it has given consumers more control, among other things by allowing them to select alternative search engines and web browsers instead of default providers. For competitors, the DMA has allowed better interoperability with gatekeepers' operating systems, for example by enabling the launch of alternative app stores. Gatekeepers must now make it easier for users to choose a default browser other than, say, Google's Chrome for Android and Safari for Apple devices. Alternatives such as Opera and Firefox have indeed seen a significant increase in active users on iOS since the DMA entered into force. At the same time, Google Chrome and Apple Safari have continued to hold stable market shares of around 60% and 30% in the European mobile browser market, respectively, since 2024. This example shows that choices have improved for consumers, but market structures remain largely unchanged.

With regard to regulating US Big Tech's conduct overall, the results have been similarly modest. The DMA's goal is for gatekeepers to behave in a way that is fair and enables competition. The DSA is intended to make large platforms tackle the risks they pose to individuals and society. Both established ex-ante obligations that Big Tech companies have had to comply with since 2024. However, fundamental concerns over Big Tech conduct persist. The number of proceedings[8] under the DMA and DSA, the recurrence of similar concerns, and legal challenges to Commission decisions indicate a reluctance to comply in full. US Big Tech appears to be pursuing a strategy of targeted adjustments, while resisting changes that would materially weaken their underlying ecosystems or business models. This practice has been labelled "malicious compliance". In the DMA review, non-gatekeeper businesses have complained about gatekeepers using delaying tactics, circumventing obligations and making design choices in that undermine their effect.

8 See table attached.

For example, Apple had adjusted its business terms to reflect the DMA's "anti-steering" obligations, which requires platforms to let business customers direct users to cheaper offers. But, as the Commission found, Apple did so in such a restrictive way that it amounted to non-compliance. Similarly, the DSA so far has not prompted Big Tech to implement meaningful changes to address issues such as addictive design. Platforms have obstructed the effective application of the DSA, including for example by delaying procedures and providing incomplete data in response to researchers' data access requests.

The inconsistent enforcement of digital rules at national level adds to the problem. The instruments discussed here are mainly enforced by the European Commission. But overall, the enforcement of digital rules is carried out by at least 300 different authorities at national and EU level, which has led to inconsistencies in their application. The GDPR in particular, mainly enforced by national authorities, has been underenforced. It has consequently done little to change how Big Tech companies collect and use European data, often a central element of their business model. Ireland's data protection authority is the lead enforcement agency for those Big Tech companies that have their European headquarters in Ireland.[9] The country is heavily dependent on tax revenues from foreign companies. In 2024, almost 40% of Ireland's total corporate tax revenues came from Apple and Microsoft alone. Ireland's data protection authority and its reluctance to rein in Big Tech has been the subject of long-standing criticism: Decisions take years, are dismissed without resolution in 99.9% of cases or in end amicable settlements. In 2023, the Irish Data Protection Commission (DPC) even sued the European Data Protection Board after it issued a binding decision to investigate Meta's handling of personal data. While this might be the area of most glaring underenforcement and political influence, the US government's threats to pressure member states, the European Commission and even individual officials, especially over the application of the DSA, have also led to concerns over the independence of the Commission's enforcement.

The dynamics in evolving markets suggest that Big Tech's business strategy continues to work. The AI and cloud markets offer further indications that the EU's regulatory interventions have not changed how US Big Tech companies work to create and entrench their dominance. Through partnering with and investing early in companies like OpenAI and Anthropic, they have been able to consolidate their position in the newest frontier of digital power, the AI market. In a familiar pattern to create lock-in effects and leverage their existing ecosystem, platforms have integrated AI into their core services, such as Google with AI Search overviews. Meta sought to exclude third-party AI assistants from WhatsApp until the Commission objected to this. Given already high barriers to entry in the AI market, these strategies make it even more difficult for smaller firms to compete. This could ultimately result in a highly concentrated market, despite DMA and competition law obligations. With the broad adoption of AI systems, there has been increasing demand for cloud services as they can provide the computing power, storage and data-processing capacity AI systems require. Here, US Big Tech companies have achieved dominant positions as well. Amazon, Microsoft and Google share around 70% of the European cloud market and can use this position to bundle cloud services with their proprietary AI models.

9 Google, Apple, Meta and Microsoft. Amazon has its headquarter in Luxembourg.

More consistent and credible enforcement is needed

If the EU wants to limit US Big Tech power, its regulatory interventions need to have more bite. It would be overly optimistic to assume that the DMA and DSA will produce more substantial change simply given more time. The more likely outcome is a continuation of the status quo: US tech firms dominate digital markets and profit from their ecosystems, enabling them to control technological developments and new frontiers. While the EU might be able to replace foreign providers for some of the services that pose security risks, it would likely continue to be dependent on US companies for the majority of its digital services without meaningful control over how those services are provided. The consequences for its economy and democracy, outlined above, would persist. If the EU wants to change this trajectory, the rules need to be enforced more effectively now.

There are three areas for action to achieve this. To level the playing field, structural remedies, stricter merger control and fairer taxation are necessary, behavioural obligations must be implemented swiftly and substantively, and enforcement gaps must be closed. Overall, the EU must acknowledged that the concentration of economic power in digital markets and the resulting societal and political power in the hands of private companies goes far beyond that of other industries – a scale that must be reflected in the EU's response to the issue.

1. Leveling the playing field through structural interventions

To address structural competition problems, structural remedies are necessary. Effective pro-competitive interventions are central to tackling Big Tech's source of power. Competition authorities can choose between different types of remedies, behavioural and structural, where dominant companies behave anticompetitively. Behavioural remedies address how a company operates, for example by requiring it to provide competitors with non-discriminatory access to infrastructure or technology. Structural remedies alter the company or the market itself, for example by requiring it to divest assets or separate business units. The Commission has not relied on structural remedies in any of its DMA decisions[10] and in none of the competition cases decided in the past six years. The DMA provides for them only as a last resort. Similarly, in the EU's antitrust enforcement, structural remedies can only be imposed if there is no equally effective behavioural remedy. It is often argued that structural remedies are more invasive than behavioural remedies. But placing more and more behavioural obligations on gatekeepers also amounts to a heavy intervention in companies' economic freedom. If other remedies have been futile and the issues persist, structural remedies are necessary.

Structural remedies are often more effective at restoring competition and easier to implement. A study by the Commission on its antitrust remedies across sectors and over 20 years found that behavioural remedies were much more ineffective than structural remedies. While structural remedies were consistently implemented and generally worked to correct markets, behavioural remedies were often weakly enforced and require constant monitoring. Around two-thirds failed to achieve their intended effects fully. In digital markets where Big Tech firms have built self-reinforcing ecosystems, structural remedies are a necessary element of pro-competitive interventions. Concretely, the Commission could impose a structural remedy, such as selling parts of its advertising business, in its AdTech case against Google. Discussions on appropriate remedies are

10 With the exception for Google's AdTech case where divesture is still a possibility.

currently ongoing.

To limit Big Tech's ability to accumulate more power through acquisitions, the EU should strengthen its merger-control framework. Effective merger control can prevent additional competition problems from arising in the first place, including through structural remedies which are more frequently used here than in antitrust cases. Blocking a merger is also arguably a less intrusive step than reversing that decision later on. To intervene in a merger, the Commission currently has to prove that a concentration will have anti-competitive effects. In digital markets, it is especially difficult to anticipate how markets will evolve, and competition authorities often lack the necessary information. This has likely led to underenforcement of the rules, as a recent study by the Commission indicates. While not every acquisition of a start-up by a Big Tech company automatically has anti-competitive effects, more scrutiny could meaningfully improve competition issues in digital markets. The Commission is currently revising its merger guidelines and plans to update them by the end of the year. This is an opportunity to adopt stricter rules for acquisitions by Big Tech companies, for example by reversing the burden of proof on companies to demonstrate the expected effect on competition. This could also be achieved by amending the DMA, giving the Commission more power to review any acquisition by gatekeepers.

Fair taxation is necessary to level the playing field. As multinational companies, US Big Tech companies have been successful in shifting their profits to countries with low taxes. In a recent compliance report, Microsoft said it earned almost 40% of its pretax income in Ireland, which has among the lowest corporate tax rate in the EU. In high-tax Germany, by contrast, Microsoft claims to have earned less than 0.5% of its global profits. In 2018, the European Commission presented a digital tax package with a 3% levy on certain digital revenues that aimed to ensure digital companies would face taxation on par with traditional companies. Member states failed to reach the unanimity required in the Council to pass the package. Negotiations then focused on reaching a global tax agreement in the OECD forum, but its implementation is stalling as the US government withdrew support. In 2021, the Commission proposed a new plan for a digital services tax to become an EU own resource, which could have contributed up to 20% of the EU's budget and helped to repay Covid recovery funds. This plan, however, was contingent on the OECD tax agreement coming into effect. Some EU member states have since introduced national digital services taxes instead, but the EU-wide initiative remains on hold. While tech companies appear to largely pass such taxes on to businesses and consumers, Big Tech companies would be more likely to actually carry a profit-based charge such as the one proposed by the OECD.

2. Effectively changing conduct

Where US Big Tech provides essential digital infrastructure in Europe, the EU should be able to set and enforce rules for their conduct. The powerful position those companies hold warrants close scrutiny. To be effective, however, compliance with the various rules the EU has set must be strengthened. The European Commission usually relies on fines and an obligation for US Big Tech to take measures that end the infringement in question. Both could have more bite.

Behavioural remedies must be implemented faster and more consistently. The ineffectiveness of remedies has been a long-standing issue in competition policy, the same problems now seem to stand in the way of the DMA and DSA taking full effect. Just as the Commission monitors the implementation of *ex-ante* obligations, it also needs to

monitor the design of remedies Big Tech platforms offer to ensure they actually work. This must be done in a timely manner so that the breach of obligations is quickly remedied The DMA and DSA proceedings were intended to produce quicker results rather than lengthy competition cases. But under the DMA, the Commission's decision on Google's self-preferencing took more than two years. And despite the closure of a 60-day window for compliance, a recent study shows that Google still prioritizes its own shopping service, meaning there has been no improvement since the start of the proceedings, and European businesses continue to be disadvantaged. Under the DSA, preliminary findings for some of the suspected breaches by Facebook and Instagram were published after 17–25 months, but there has been no non-compliance decision or fine as yet. Where breaches are clear, the regulatory response needs to be quicker.

Both under the DSA and the DMA, the Commission has the power to apply interim measures. They can be applied in urgent cases where there is a risk of serious damage to businesses or users. The Commission has not yet made use of these powers because the bar to prove "risk of serious damage" is relatively high. Interim measures have also hardly ever been used in competition proceedings. To make the Commission's interventions meaningful and not repeat the same shortcomings of competition proceedings in digital markets, interim measures should be on the table.

Despite claims that the EU is regulating Big Tech too "aggressively", in reality, fines have been modest. Although more than €20 billion in fines over six years may seem like a lot, they are likely not high enough to have the intended deterrent effect for a group of companies with annual revenues in Europe of around €400 billion.[11] Instead, companies likely just see them as the price of doing business. The most recent DMA fine against Google of €890 million only amounted to 0.25% of the annual revenue of parent company Alphabet. Previous fines against Apple and Meta came to 0.14% and 0.13%, respectively. In total, the Commission fined €1.59 billion where the maximum possible would have been around €123 billion. Even if the newness of the laws, the short duration of the breaches and other factors are taken into account, these fines are rather modest. To ensure a deterrent effect, higher fines are necessary.

3. Tackling enforcement gaps

With an increasingly complex digital rulebook, the EU needs to improve its enforcement structure. The EU has built an extensive digital rulebook over the last few years. But the issue is not necessarily that Big Tech's problematic practices escape these rules. Instead, the problem is the lack of effective enforcement. There is currently no forum for different competent authorities to exchange information or coordinate enforcement at EU level. This leads to inconsistency, delays and duplications in applying European digital laws, and is further exacerbated by the fact that many enforcement authorities are under-resourced, in particular lacking staff. The European Commission, the primary enforcer of digital rules against Big Tech, has further proven susceptible to political pressure from the US government by delaying several DMA decisions. This is a risk to its credibility as an enforcer and could lead to over- or underenforcement.

Many different options to address this "enforcement gap" have been discussed. They propose varying levels of independence, from merely improving coordination and setting up an information sharing forum to establishing an independent authority like the European Central Bank or an agency such as the Anti-Money Laundering Authority. However, there are legal hurdles to overcome and also likely higher costs than keeping

11 Assuming around 20-25% of global revenue in Europe.

enforcement within the Commission. In addition, given the resources and political power of Big Tech companies, holding them accountable may require an institution with the authority and political weight of the European Commission. In any case, better coordination mechanisms and sufficient resources would be viable steps to improve enforcement.

To enforce the GDPR, the European Commission and member states should put more pressure on Ireland. At European level, there are limited ways to force the Irish DPC, or other national data protection authorities, to take action. In theory, the Commission could open an infringement procedure against Ireland for failing to put adequate enforcement policies in place. However, a complaint filed by an NGO to trigger such an infringement procedure in 2021 only ended in a decision by the EU Ombudsman that the Commission must adequately monitor Ireland's Big Tech cases. More viable are the GDPR's monitoring and dispute resolutions mechanisms: Other member states can challenge decisions by the Irish DPC if they have relevant and reasoned objections. If the conflict remains unresolved, the European Data Protection Board (EDPB) can issue a decision that is binding on the Irish DPC. This approach has already been used several times to correct Irish decisions. The EDPB also has the power to force national regulators to open new investigations. Where national authorities undermine effective enforcement for all of Europe, these steps should be used exhaustively.

Conclusion

Europe needs to be more independent of US Big Tech companies. Its current reliance on foreign tech firms for most of its digital services comes with considerable costs and risks for the European economy, its democracy and security. In response, the EU is pursuing digital sovereignty. Whether Europe can achieve this sovereignty will depend on whether it can successfully build up European alternatives, which will require massive investments over a decade. For people to put money on the line and invest in start-ups and scale-ups, they need to be sure that there is a market to compete for. This requires a credible European regulator that puts political weight behind the creation of competitive digital markets. Without stronger enforcement, the likely outcome is continued dependence. In addition, where a complete decoupling is neither desirable nor realistic, US Big Tech companies will continue to be powerful operators in the European market. To shape its digital future, the EU has to be able to control Big Tech's behaviour in its market.

Effective tech regulation is a matter of sovereignty and should be treated as a matter of strategic priority. In her 2026 State of the Union address, Commission President Ursula von der Leyen said notably: "I am aware that many perceive the power of Big Tech as overwhelming. And impossible to roll back. I disagree." Considering the power US tech giants have accumulated, it is easy to assume they are beyond democratic control. But the EU's dependency is not entirely one-sided: Big tech needs the European market of 450 million wealthy consumers. That puts the EU in a very different position to many smaller countries that are forced to accept the conditions Big Tech companies offer – or risk that they will leave their markets. The EU should use the leverage it has to take control of its digital future, build European alternatives and hold US Big Tech accountable.

Annex: The EU's recent enforcement action against US Big Tech companies

Proceedings under the Digital Markets Act

Company	Service	Type of proceeding	Obligation	Start of proceedings	Decision date	Duration in months	Remedy	Fine in mn €
Google	Search	Compliance	Self-preferencing (Art. 6(5))	25.03.2024	23.07.2026	27	Fine, cease and desist order	460
Google	Play	Compliance	Anti-steering (Art. 5(4))	25.03.2024	23.07.2026	27	Fine, cease and desist order	430
Google	Android	Specification	Interoperability (Art. 6(7))	27.01.2026	16.07.2026	5	Specification decision	
Google	Search	Specification	Access to data (Art. 6(11))	27.01.2025	16.07.2026	5	Specification decision	
Google	Search	Compliance	Self-preferencing (Art. 6(5)), FRAND conditions for access (Art. 6(12))	12.11.2025	ongoing			
Apple	iOS	Specification	Interoperability (Art. 6(7))	19.09.2024	19.03.2025	6	Specification decision	
Apple	iOS	Compliance	App un-installation and change of default settings (Art. 6(3))	25.03.2024	23.04.2025	12	Closure, behaviour changed	
Apple	App Store	Compliance	Anti-steering (Art. 5(4))	25.03.2024	23.04.2025	12	Fine, cease and desist order	500
Apple	iOS	Specification	Interoperability (Art. 6(7))	19.09.2024	19.03.2025	6	Specification decision	
Apple	iOS	Compliance	Side-loading (Art. 6(4)), anti-steering (art. 5(4)), interoperability (art. 6(7)), tying of services (art. 5(7))	24.06.2024	ongoing			
Meta	Platforms	Compliance	Personal data processing (art. 5(2))	25.03.2024	23.04.2025	12	Fine, cease and desist order	200

Proceedings under EU competition law

Company	Topic	Obligation	Start of proceedings	Decision date	Duration in months	Remedy	Fine in mn €
Google	AI and data-related practices	Art. 102 TFEU, Art. 54 EEA	09.12.2025	ongoing			
Google	AdTech and data-related practices	Art. 102 TFEU, Art. 54 EEA	14.06.2021	05.09.2025	50	Fine, prohibition decision	2950
Apple	App Store Practices (e-books/ audiobooks)	Art. 101 TFEU, Art. 102 TFEU, Art. 53 EEA, Art. 54 EEA	16.06.2020	22.11.2024	53	Closure	
Apple	Mobile payments	Art. 102 TFEU	16.06.2020	11.07.2024	48	Commitment decision	
Apple	App Store practices	Art. 101 TFEU, Art. 102 TFEU, Art. 53 EEA, Art. 54 EEA	16.06.2020	24.06.2024	48	Closure	
Apple	App Store practices (music streaming)	Art. 102 TFEU, Art. 54 EEA	16.06.2020	04.03.2024	44	Prohibition decision	1800
Meta	Exclusion of AI competitors from WhatsApp	Art. 102 TFEU, Art. 54 EEA	04.12.2025	09.06.2026	6	Interim measures	
Meta	Facebook Marketplace	Art. 102 TFEU, Art. 54 EEA	04.06.2021	14.11.2024	41	Fine	797
Microsoft	Teams II	Art. 102 TFEU, Art. 54 EEA	25.06.2024	12.09.2025	14	Commitment decision	
Microsoft	Teams	Art. 102 TFEU, Art. 54 EEA	27.07.2023	12.09.2025	25	Commitment decision	
Amazon	Buy Box	Art. 102 TFEU, Art. 54 EEA	10.11.2020	20.12.2022	25	Commitment decision	

Overview of DSA proceedings

Company	Service	Obligation	Start of proceedings	Preliminary findings	Final decision date
Meta	Facebook	Art.14(1), 16(1), 16(5), 16(6), 17(1), 20(1), 20(3), 24(5), 25(1), 34(1), 34(2), 35(1) and 40(12)	30.04.2024	24.10.2025	ongoing
Meta	Facebook	Art. 28, 34, and 35	26.05.2024	29.04.2026	ongoing
Meta	Facebook	Art. 28, 34, and 35	26.05.2024	10.07.2026	ongoing
Meta	Instagram	Art.14(1), 16(1), 16(5), 16(6), 17(1), 20(1), 20(3), 24(5), 25(1), 34(1), 34(2), 35(1) and 40(12)	30.04.2024	24.10.2026	ongoing
Meta	Instagram	Art. 28, 34, and 35	26.05.2024	29.04.2026	ongoing
Meta	Instagram	Art. 28, 34, and 35	26.05.2024	10.07.2026	ongoing

Overview of GDPR fines issued by lead enforcement agencies

Company	Authority	Topic	Obligation	Date	Fine
Google	Ireland	Insufficient legal basis for data processing	Art. 5, Art. 6, Art. 12, Art. 13	21.09.2026	403
Meta	Ireland	Insufficient technical and organisational measures to ensure information security	Art. 33 (3), (5), Art. 25 (1), (2)	17.12.2024	251
Meta	Ireland	Insufficient technical and organisational measures to ensure information security	Art. 5 (1) f), Art. 32 (1), Art. 33 (1), (5)	27.09.2024	91
Meta	Ireland	Insufficient legal basis for data processing	Art. 46 (1)	12.05.2023	1200
Meta	Ireland	Non-compliance with general data processing principles	Art. 5 (1) a), Art. 6 (1), Art. 12, Art. 13 (1) c)	04.01.2023	390
Meta	Ireland	Insufficient technical and organisational measures to ensure information security	Art. 25 (1), (2)	25.11.2022	265
Meta	Ireland	Non-compliance with general data processing principles	Art. 5 (1) a), c), Art. 6 (1), Art. 12 (1), Art. 24, Art. 25 (1), (2), Art. 35	05.09.2022	405
Meta	Ireland	Insufficient technical and organisational measures to ensure information security	Art. 5 (2), Art. 24 (1)	15.03.2022	17
Meta	Ireland	Insufficient fulfilment of information obligations	Art. 5 (1) a), Art. 12, Art. 13, Art. 14	02.09.2021	225
Amazon	Luxembourg	Personal data processing	-	16.07.2021	0 (annulled)
Microsoft	Ireland	Insufficient legal basis for data processing	Art. 5 (1) a), Art. 6 (1) a), e), f), Art. 13 (1) c), Art. 14 (1) c)	24.10.2024	310

Gefördert durch:

Bundesministerium der Finanzen

Hertie School gGmbH • Chairman of the Supervisory Board: Frank Mattern • Chairman of the Board of Trustees: Prof. Dr. Helge Braun • Managing Director: Dr. Axel Baisch • Registered Office: Berlin • Trade Register: Local Court, Berlin-Charlottenburg HRB 97018 B • Hertie School – founded and supported by the non-profit Hertie Foundation

Friedrichstraße 180
D – 10117 Berlin
Tel.: +49 (0)30 259219-339

Online: delorscentre.eu
E-Mail: info@delorscentre.eu
Bluesky: delorsberlin.bsky.social