

BREXIT & DIGITAL REGULATION

Regulating the Digital Sphere after Brexit

Ten years on, the UK and the EU have built broadly parallel rules for personal data, digital markets and online safety — converging in substance despite divergent rhetoric. Artificial intelligence remains the sharpest divergence, even as shared US pressure pushes the two closer together.

Antoine Cèbe

Executive Summary

Ten years after Brexit, the EU and the UK have adopted broadly parallel legislation governing the digital economy. Despite differing rhetoric, London emphasising innovation, Brussels prioritising rights, the legal rules converge across four domains. On personal data, the UK retained a lightly amended GDPR and secured a renewed EU adequacy decision in December 2025. On digital market competition, the EU's Digital Markets Act (2022) designates “gatekeepers” and imposes ex ante obligations, while the UK's DMCC Act (2024) empowers the CMA to set case-by-case rules; both carry fines of up to 10% of global turnover. On online safety, the EU's Digital Services Act and the UK's Online Safety Act share the same logic of tiered obligations, with the UK setting a 10% fine ceiling versus 6% for the EU.

The sharpest divergence lies in artificial intelligence. The EU adopted a comprehensive, horizontal AI Act in 2024; the UK initially chose not to regulate but has since signalled its intention to act on the most powerful models. This gap may narrow as Brussels reconsiders implementation and London moves toward sector-specific rules.

On the US front, a February 2025 White House memorandum and a House Judiciary Committee investigation targeted both British and European digital legislation, accusing them of “seizing” US tech company revenues. This shared pressure reinforces the UK-EU alignment and has underpinned a bilateral cooperation agreement on competition (April 2026). For businesses, the remaining legislative divergences create non-tariff barriers, and the comparative advantage the UK derives from its lighter regulatory framework does not appear to offset the compliance costs for firms exporting to the EU.

Introduction

Ten years after Brexit, the European Union and the United Kingdom have adopted new legislation governing digital life and the digital economy. Data protection, the digital economy, online safety and artificial intelligence are all domains in which Brussels and London are developing broadly similar regulatory tools. This British alignment with the European approach reveals the shared interests of the two trading partners and confirms their rapprochement.

On both sides of the Channel, the digital sphere is a major economic and social issue. A point of geopolitical tension with the United States, British and European regulatory choices are broadly aligned. While London projects a pro-innovation discourse and Brussels one of rights protection, the legal rules ultimately chosen trace a common direction. The European Union has opted for substantive and procedural rules defined ex ante, grounded in several legislative interventions across personal data protection, online safety, the digital economy and artificial intelligence. The Westminster legislature has intervened in the same domains, with similar objectives and a broadly similar method. On personal data protection, the United Kingdom has retained the European framework with minor adaptations. British online-safety regulation is fully aligned with the European method, with a broad scope of obligations and rules defined ex ante; it remains more limited on consumer protection and more extensive on the protection of minors and age verification. The third country's intervention in the digital economy pursues the same objectives as the European Union's, but unlike Brussels, London has chosen to define rules ex post, in a targeted manner for each regulated firm, following a market investigation. While this approach may appear more precise and effective, it also requires more time to impose obligations that may ultimately mirror those of the European Union. Artificial intelligence is the domain where the United Kingdom and the European Union diverge. The United Kingdom chose not to regulate the technology through ad hoc legislation, whereas the European Union has equipped itself with a comprehensive framework. This difference in approach may narrow as the European Union steps back on implementation and the British government signals its intention to regulate firms deploying the most powerful AI models.

Beyond the rhetoric, the shared challenges facing the European Union and the United Kingdom in the digital field have prompted a broadly similar approach to data protection, online safety and the digital economy — and perhaps, before long, to artificial intelligence.

1. The Shared Challenges of the European Union and the United Kingdom

In a clear break with the Conservative Party line, British Prime Minister Keir Starmer announced in January 2026 his intention to align with the EU's single market against a backdrop of shifting international relations. President Donald Trump had directly attacked both British and European digital legislation in the same salvo. He accused London and Brussels of seizing the revenues of US tech companies through discriminatory regulation. Yet when withdrawing from the EU, the UK had publicly aspired to become "the new European Singapore". The country was to constitute an economic zone wide open to trade, and commercial freedom would provide a competitive edge in global markets. In 2016, the UK exported roughly 40% of its goods and services to the EU. That remains true ten years later. An indispensable market for British digital companies, the UK oscillates between offering a regulatory framework attractive for innovation and competitiveness and aligning its standards with the EU. Faced with the EU's preventive, horizontal model of digital economy regulation, the UK pursues a more targeted approach which, in theory, is advocated as more innovation-friendly. These regulatory differences create non-tariff barriers to entry into European digital markets.

The British digital economy faces challenges similar to those of the EU. The sector accounts for a significant share of national output. In 2023, the digital sector represented approximately 5.2% of value added in the EU and around 6.5% of value added in the UK. It also carries major risks: economic concentration of markets, online violations of individual rights, and threats to democratic life. In response, the EU and the UK have developed a new legislative arsenal in recent years, the latter following the former's lead. The new rules address the key issues of digital economy regulation: cybersecurity, online data protection, competition between digital market players, online consumer protection, safeguarding democracy online, and promoting business competitiveness

and innovation. Since the end of EU law's applicability in the UK, successive Conservative and Labour governments have broadly supported this regulatory movement. While the Conservative Party's policy was one of gradual divergence from European norms, the Labour Party, in power since July 2024, was elected on a platform explicitly favouring rapprochement with the EU. This commitment culminated in the first UK-EU summit since Brexit in May 2025, under the banner of "reset".

Ten years after Brexit, the UK is choosing to progressively rebuild its relationship with the EU. This rapprochement, grounded in regulatory alignment, demonstrates a community of interest that did not disappear with the UK's departure. Personal data, the digital economy, online safety and artificial intelligence are all regulatory domains that illuminate both the extent and the limits of this alignment.

2. Online Personal Data: Between Innovation and Protection

The UK first preserved the EU's personal data protection framework. Personal data refers to all traces that an individual leaves online and that can be used to identify them. The EU's General Data Protection Regulation (GDPR), which entered into force in 2018, established the first substantive regulatory framework for the use of personal data in the digital economy. The text was a compromise. The EU sought a harmonised legal framework across Europe to prevent diverging national laws from hampering the growth of a digital economy now built on mass data processing. A degree of liberalisation of personal data sharing is at work, but the text remains centred on the right to privacy. Yet access to individuals' personal data also creates new dangers for citizens' security and their freedom of choice.

In 2018, the "Cambridge Analytica" scandal broke: a British company was accused of illegally harvesting the personal data of 87 million Facebook users and providing profiling services to the Trump campaign and to pro-Brexit parties ahead of the UK referendum. While the actual effects of this activity on the outcomes of those two democratic events remain debated, the importance of online data protection for British citizens was laid bare, revealing the need to further safeguard citizens' right to privacy online. Under the GDPR, any entity that collects or processes personal data within the EU must comply with a set of obligations designed to protect the rights of the individuals whose data it uses. These obligations apply to data processing companies operating within the single market and when exporting data outside it. The GDPR supplements the 2002 European "e-Privacy" Directive, which also governs personal data processing in the electronic communications sector. After its withdrawal from the EU on 31 December 2020, the UK retained the EU secondary law adopted before its departure. Accordingly, both European online privacy laws were transposed into UK domestic legislation.

In 2021, Prime Minister Boris Johnson's government announced its intention to amend the legislative framework. The goal was to "unlock the power of data" as part of the Conservative government's "technological golden age" strategy. With the Data Protection and Digital Information Bill introduced in 2023, the government sought to significantly ease online data protection rules and facilitate data processing by businesses. Abandoned after the 2024 general election, the Labour majority proposed a new version of the reform: the Data (Use and Access) Bill 2024-25. Adopted in June 2025, the reform does not replace the GDPR but amends it. The text represents a more modest overhaul of the existing framework.

This more cautious stance preserves the renewal of the European Commission's adequacy decision while easing GDPR constraints. This decision recognises the equivalence of online personal data protection levels in the UK and the EU. The former member state had benefited from it since 2021. Personal data transfers between the two territories are therefore not subject to additional rules applicable to third countries. A key issue for the digital economy, losing this benefit would seriously impede UK-EU trade in this area. While the Commission's

adequacy decision was due to expire in June 2025, the Commission extended the initial decision until the adoption of the British reform. A second adequacy decision was finally granted in December 2025, following review of the British reform. The new legal framework aims to promote innovation and provides for eased obligations on companies regarding personal data processing. Whether such easements will actually benefit British companies, or whether the importance of EU trade will push them to maintain full GDPR-compliant procedures, remains to be seen.

3. A European and British Movement to Regulate the Digital Sphere

On 21 February 2025, the White House published the memorandum “Defending American Companies and Innovators From Overseas Extortion and Unfair Fines and Penalties,” addressed to the Secretary of the Treasury and the Secretary of Commerce. The memorandum aimed to defend US tech companies against the “seizure” of their revenues by foreign states through discriminatory digital services regulation. While digital services taxes and “costly” regulation were specifically targeted, President Trump also instructed the Secretaries of State to investigate any acts, policies or practices by EU member states or the UK that would require or encourage US companies to operate in ways that infringe freedom of expression and political engagement. Following US Vice President J.D. Vance’s speech at the Munich conference on 14 February 2025, the House Judiciary Committee opened an investigation into EU digital regulation on the same grounds, on 23 February 2025.

Through these actions, the United States signalled its opposition to the legislation enacted in the UK and by the EU to constrain the power of large tech companies and regulate online life. Guilty of anti-competitive behaviour, the major digital companies also carry numerous ills: online hate, harassment, diffusion of violence, opinion manipulation and disinformation. They are few in number, most often foreign-owned, and hold nearly all market share in digital economy sectors. On both sides of the Channel, governments seek to regulate online spaces to make them safer and to restore effective competition in digital markets. Confronted with the limits of competition policy, the EU adopted the Digital Markets Act (DMA) in 2022. In a parallel move, the UK adopted the Digital Markets, Competition and Consumers Act (DMCC) in 2024. Likewise, as general law proved insufficient to regulate digital services, the EU enacted the Digital Services Act (DSA) in 2022. The UK responded with the Online Safety Act in 2023.

4. The Alignment of Digital Economic Regulation

The UK and the EU both seek to deconcentrate digital markets. This is not merely a question of digital sovereignty but also of competitiveness for British and European firms. When a handful of private actors control the diffusion of innovation in digital markets, set prices and dictate the terms of commercial relationships, they subordinate European businesses to their decisions. Competition in digital markets is particularly weak given the concentration of market share among a few companies. EU competition policy has proven insufficient to address this situation. Competition policy aims to ensure that firms compete for market share. This pressure is meant to make them more competitive, more innovative, and to generate beneficial effects for consumers. To deter companies from colluding to carve up markets, or a dominant firm from abusing its position to eliminate competitors, the EU sanctions anti-competitive behaviour and reviews mergers. But enforcing these powers takes considerable time, poorly suited to digital markets, and sanctions are ineffective against companies with vast cash reserves.

The EU’s competition offensive began in 2004 with an initial decision against Microsoft and has continued to this day. Between 2004 and 2025, the European Commission adopted around twenty competition infringement

decisions against the GAFAM, with the pace accelerating from the 2010s onward. Despite these sanctions, the market power of the few companies dominating digital markets has continued to grow. Between 2010 and 2019, GAFAM market capitalisation surged dramatically: Facebook's market capitalisation, the lowest of the five, was for instance three times higher than those of Exxon, Nike or Coca-Cola. The EU therefore chose to regulate large tech companies to compel them to adopt certain practices and to enable the deconcentration of digital markets.

The Digital Markets Act (EU)

The Digital Markets Act (DMA) entered into force in Europe in 2023. It equips the European Commission with tools complementary to competition law. The DMA allows the Commission to designate firms as “gatekeepers” of digital markets. The designated gatekeepers since 2024 are Alphabet, Apple, Meta, Amazon, Microsoft, and ByteDance. Their services are ubiquitous in the daily lives of businesses and citizens: Google Chrome, iOS, Instagram, WhatsApp, Windows and TikTok, among others. The DMA sets out a series of obligations and prohibitions for these companies regarding the use of and access to data collected through their digital services, the distribution of their digital services and the interoperability of their services. Gatekeepers must, for example, allow the installation of third-party “software applications” within an operating system. In practice, this means that Apple must allow the installation of applications such as a browser, a messaging app or an app store within the iOS operating system powering iPhones.

The aim is to give application developers the ability to compete with the firm in the native app market by prohibiting the closure of the Apple ecosystem. Gatekeepers must also ensure the interoperability of online messaging services. Ultimately, Meta will have to offer users of WhatsApp and Telegram, a competing messaging service, the ability to exchange messages across their respective applications. The objective is to limit the network effects generated by these services. The more users a messaging application has, the more indispensable it becomes. Users must therefore be freed from captivity to a single messaging network.

The Digital Markets, Competition and Consumers Act (UK)

Following the DMA's lead, the British Digital Markets, Competition and Consumers Act (DMCC) pursues the same overarching goal: regulating competition in digital markets. The Act entrusts this mission to the UK's competition authority, the Competition and Markets Authority (CMA). Like the European Commission, the CMA can designate certain digital economy firms as holding “strategic market status”. These designated firms will be subject to specific obligations. Unlike the EU's DMA, the UK text does not set out obligations or prohibitions as such but rather empowers the competition authority to define obligations on a case-by-case basis for each designated firm. These new rules will likely be similar to those established by the EU, given that market structures are broadly the same. While the DMA has been fully applicable since 2024 on the European side, the British authority must still craft these rules to meet the Act's objectives. The CMA designated Google and Apple for various digital services in October 2025. However, after initially announcing certain behavioural obligations regarding both companies' app stores, the CMA ultimately abandoned the imposition of mandatory measures, preferring to rely on commitments from the two firms.

Both companies committed to treating competing applications fairly and transparently within their app stores. Apple committed not to arbitrarily refuse a developer the ability to distribute an application on the App Store in order to protect its own native applications. The CMA also submitted for public consultation proposed behavioural obligations on Google in February to allow online content producers to control how Google uses their content for its artificial intelligence services. An investigation into whether to designate Microsoft is ongoing. In case of non-compliance, both the European Commission and the CMA can impose fines of up to 10% of the firm's global annual turnover. Alphabet's global revenue in 2025 was \$402.8 billion. Ten per cent of that

figure, converted to euros, represents just under €35 billion, slightly more than 1% of French or British GDP in 2025. These amounts are comparable to those under competition law, and the fines actually imposed are typically much lower. The European Commission has already sanctioned some of the designated companies: Apple was fined €500 million and Meta €200 million in April 2025.

The EU adopted a less flexible and more prescriptive approach than the UK to complement its competition policy, but the spirit of both texts is the same. The Commission enforces behavioural obligations defined by the European regulation, while the CMA may define bespoke behavioural obligations based on its market investigation findings. While both methods pursue the same results, it will be possible only in retrospect to judge which proves more effective. On both sides of the Channel, governments want competition authorities to structurally open markets and constrain the behaviour of multinationals. These shared objectives are underpinned by a bilateral cooperation agreement on competition concluded in April 2026. While the simplification agenda has touched EU digital legislation, UK competition policy is subject to a pro-innovation and pro-industry discourse pushing it toward a degree of relaxation, notably in merger control. The appointment of Doug Gurr as CMA Chair in January 2025 is telling, the new chair had served as Amazon UK President from 2016 to 2020. Whether differences in the profiles of those leading regulatory authorities will produce a change of policy in this area remains to be seen.

In a joint offensive on the digital economy, London and Brussels have also intervened to protect online users. Citizens, children and consumers are targets of attacks that governments seek to curb.

Securing Online Spaces: Two Methods, One Goal

The EU and the UK seek to make online life safer and to regulate the negative effects of digital services on society. While the extent of digital services regulation varies across domains between the two legal orders, British and European legislation adopts a broadly similar approach. Both Brussels and London have entrusted independent authorities with regulating tech companies on issues including illegal content, online child protection, consumer protection and democratic life online. European and British legislation is prescriptive. Both require online platforms, social networks and search engines to act at the level of both service design and operation. If a user is harassed on Facebook, Meta must act promptly. If a child uses Google Chrome, they must not be exposed to pornographic content. An election must not be threatened by waves of disinformation or hatred directed at candidates. X must be compelled to act if the service is used for terrorist activities. Amazon must act if an online seller defrauds consumers. Both the UK and the EU chose to regulate online life broadly through the Digital Services Act and the Online Safety Act. Their chosen response is to hold tech companies accountable. The EU and the UK now officially cooperate on the implementation of this policy.

The Digital Services Act (EU)

On the European side, the Digital Services Act entered into application in 2023. It launched a policy of digital services regulation. The aim is to ensure that users' online lives take place in a "safe online environment", or at least one safer than at present. The text creates new rules to constrain the power of digital companies, with several cumulative layers. Some rules apply to all digital companies that enable the sharing or storage of information online. Additional rules apply cumulatively to hosting services, online platforms and very large search engines and online platforms. The logic of asymmetric regulation based on a firm's market position or size, already present in the DMA, is replicated here. In practice, the Commission designated as very large search engines or very large online platforms Alphabet, Amazon, Apple, Meta, Microsoft, X, TikTok, Booking, and Wikipedia, as well as Aylo, WebGroup and Technius, in 2023.

The new rules aim to ensure transparency in terms of service and in decisions to restrict a user's access to the service; to create mechanisms for reporting illegal content and for appealing company decisions; to ensure effective consumer protection; and to broadly safeguard online environments and their harmlessness to civic processes. For example, very large digital companies designated on the basis of their large user bases must mitigate the risks their services pose to electoral processes or public security. The role assigned to large digital companies in safeguarding online environments goes beyond purely economic or consumer-protection issues, extending to the functioning of European democracies. The European Commission plays a central role in the implementation of this regulation, acting alongside national regulatory authorities. In France, the *Autorité de régulation de la communication audiovisuelle et numérique* (Arcom) is responsible for enforcement. The Commission has already launched investigations and sanctioned several companies. X was fined €120 million in December 2025. Whaleco Technology (Temu) was fined €200 million in May 2026.

The Online Safety Act (UK)

The Online Safety Act began entering into application in the UK in December 2024. Its ambition is similar to the DSA's: to make Internet use safer. The method differs. The Act contains fewer obligations and prohibitions. It creates a duty of care that must be observed by all user-to-user services and search engines. This duty of care varies according to the type of service, its number of users and the nature of the risk to users. All covered companies must assess the risks their services pose with respect to illegal content that may be disseminated through them and implement proactive measures to detect and remove illegal content through reporting and complaints mechanisms. In doing so, they must take into account users' freedom of expression and right to privacy. Companies must also integrate child protection measures against harmful content (that is, legal content that may harm a child user).

All pornography distribution services must implement age verification measures. In addition to this general duty of care, the Act creates three additional categories of companies covering social networking services, search engines and messaging applications. The companies concerned are targeted based on their size and the nature of their services. These three categories are subject to additional obligations regarding transparency, particularly concerning risks to children, risk assessment, protection of journalism and political debate, age verification and advertising fraud prevention.

While the DSA has been fully applicable since 2024, the OSA is being phased in from December 2024 and is expected to be fully applicable by 2027. The obligations to implement the general duty of care and the child online protection requirements are now in force; the additional regimes for the three specific categories of companies are not yet in place. Ofcom, the UK communications regulator, is the designated authority for enforcing the Act. The sanctions the authority may impose reach 10% of the offending company's global annual turnover, compared to 6% of global turnover under the DSA.

5. Significant Divergences on Artificial Intelligence

Artificial intelligence is the area where the UK and the EU differ most. The EU adopted the AI Act in 2024. The text sets out a series of obligations for risk assessment and mitigation, perceived as constraints on innovation. The European approach applies horizontally to all AI companies regardless of size, with requirements varying according to the degree of risk to user safety. The approach appears relatively straightforward, but the text has proven highly complex to implement, and the rules may already be obsolete given the evolving nature of the technology. Brussels has begun to backtrack in order to protect innovation. The UK initially chose not to regulate this technology as such, stating its preference for applying existing law to different use cases, before announcing its intention to regulate the most powerful models. While the British government was still shaping its doctrine, London established itself as one of the world's leading AI hubs. The government's approach is resolutely pro-innovation, and the UK has launched an industrial innovation policy in the field, supported notably by strong public demand. Yet the social effects of AI prompted a desire to regulate the technology following the Grok affair. In January 2026, X's AI sparked outrage over a feature allowing users to digitally undress images of people found online. The government signalled its intention to act, although concrete measures have not yet been taken.

Aligned Values and Objectives, Different Methods

Since the UK's departure from the EU, London and Brussels have adopted a broadly similar approach to the regulation of digital life and the digital economy. They impose obligations of varying stringency on digital companies according to their size and position in the digital economy.

Institutional Implications

From an institutional standpoint, this alignment of values and objectives enables a rapprochement that is only just beginning. While both London and Brussels have opted to define more or less precise rules on online safety and the digital economy, both legal orders have granted regulators substantial discretion to adapt these rules to technological and economic developments. Facing broadly similar challenges, London and Brussels have every interest in deepening their cooperation in this area, particularly at a time of upheaval in global trade.

Implications for Business

For European and UK businesses, while the approaches are broadly similar, subtle and often complex legislative divergences create legal uncertainty and non-tariff trade barriers that could prove harmful to the sustainability of trade between the two zones. The relative easing of innovation-related rules is of limited significance given the commercial interests at stake: the comparative advantage derived from the UK's legal framework does not appear to offset the compliance costs for exports. The conclusion of free trade agreements between the UK and third countries cannot compensate for the decline in trade growth with the European partner, since new partnerships will merely replicate those the UK already enjoyed before Brexit.

Bibliography

Agreement on the Withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community. January 24, 2020. OJ L 29/7, January 31, 2020.

Almada, M., and N. Petit. "The EU AI Act: Between the Rock of Product Safety and the Hard Place of Fundamental Rights." *Common Market Law Review*, no. 1 (2025): 85.

- Alphabet Inc. “Alphabet Announces Fourth Quarter and Fiscal Year 2025 Results.” Press release, February 4, 2026.
- Assemblée Nationale, Commission des affaires économiques. Rapport d’information sur les plateformes numériques, by V. Faure-Muntian and D. Fasquelle. June 24, 2020.
- Audureau, W. “Ce qu’il faut savoir sur Cambridge Analytica, la société au cœur du scandale Facebook.” *Le Monde*, May 16, 2018.
- Birch, Kean, and D. T. Cochrane. “Big Tech.” *Science as Culture* 31 (2022). Routledge.
- Bourreau, M., and A. Perrot. Digital Platforms: Regulate Before It’s Too Late. *Les Notes du Conseil d’Analyse économique*, no. 60, October 2020.
- C.N.I.L. “Donnée personnelle.” May 2026.
- C.N.I.L. “Royaume-Uni: la Commission européenne renouvelle ses décisions d’adéquation.” December 23, 2025.
- Castets-Renard, Céline, and Nicolas Catelan. Données à caractère personnel — Aspect pénal IP/IT. Répertoire IP/IT et Communication. Paris: Dalloz, November 2019.
- Commission Implementing Decision (EU) 2021/1772 of 28 June 2021 Pursuant to Regulation (EU) 2016/679 on the Adequate Level of Protection of Personal Data by the United Kingdom. C(2021) 4800. OJ L, June 28, 2021.
- Commission Implementing Decision (EU) of 28 June 2021 Pursuant to Directive (EU) 2016/680 on the Adequacy of the Level of Protection of Personal Data by the United Kingdom. C(2021) 4801.
- Commission nationale pour la protection des données. “Extension of Six Months of the Adequacy Decisions Allowing the Free Flow of Personal Data between the European Union and the United Kingdom.” August 4, 2025.
- Competition and Markets Authority. “CMA Confirms Apple and Google Have Strategic Market Status in Mobile Platforms.” Press release, October 22, 2025.
- Competition and Markets Authority. “CMA Launches Strategic Market Status Investigation into Microsoft’s Business Software Ecosystem.” Press release, May 14, 2026.
- Competition and Markets Authority. “CMA Secures Commitments from Apple and Google to Improve Fairness in App Store Processes and Enhance iOS Interoperability.” Press release, February 10, 2026.
- Competition and Markets Authority. “Former Amazon Boss Named Interim Chair of CMA.” Press release, January 21, 2025.
- Competition and Markets Authority. “Google’s General Search Services: Proposed Conduct Requirements.” Press release, January 28, 2026.
- Competition and Markets Authority. “Online Platforms and Digital Advertising: Market Study Final Report.” June 1, 2020.
- Conservative and Unionist Party. Manifesto 2019: Get Brexit Done: Unleash Britain’s Potential. November 24, 2019.
- Conservative Party. The Conservative and Unionist Party Manifesto 2024: Clear Plan, Bold Action, Secure Future. June 11, 2024.
- Crémer, J., Y.-A. de Montjoye, and H. Schweitzer. Competition Policy for the Digital Era. Luxembourg: Publications Office of the European Union, 2019.
- Department for Science, Innovation and Technology. “Economic Estimates: Digital Sector Annual Gross Value Added (2019 to 2023).” March 6, 2025.
- Department for Science, Innovation and Technology. “Online Safety Act: Explainer.” Guidance, April 24, 2025.
- Department for Science, Innovation and Technology. Data (Use and Access) Bill Factsheet: Growing the Economy. October 24, 2024.
- Digital Markets, Competition and Consumers Act 2024 (UK).
- Direction générale du Trésor. “Brèves numériques, Royaume-Uni.” 2026.
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 (Directive on Privacy and Electronic Communications). OJ L, July 12, 2002.
- Dommett, K. “The Inter-Institutional Impact of Digital Platform Companies on Democracy: A Case Study of the UK Media’s Digital Campaigning Coverage.” *New Media & Society*, no. 10 (2023): 2763.
- European Commission, DG for Communications Networks, Content and Technology. “Impact Assessment Report Accompanying the Proposal for a Regulation on a Single Market for Digital Services (Digital Services Act).” SWD(2020) 348

final, December 15, 2020.

European Commission. “Commission Designates Second Set of VLOPs under the DSA.” Press release, December 20, 2023.

European Commission. “Commission Finds Apple and Meta in Breach of the Digital Markets Act.” Press release, April 23, 2025.

European Commission. “Commission Fines Temu €200 Million for Breaching the Digital Services Act.” Press release, May 28, 2026.

European Commission. “Commission Fines X €120 Million under the Digital Services Act.” Press release, December 5, 2025.

European Commission. “Communication on the European Democracy Action Plan.” COM(2020) 790 final, December 3, 2020.

European Commission. “Simpler EU Digital Rules and New Digital Wallets to Save Billions for Businesses.” Press release, November 19, 2025.

European Commission. “White Paper: On Artificial Intelligence — A European Approach to Excellence and Trust.” COM(2020) 65 final, February 19, 2020.

European Commission. Antitrust and merger decisions in digital markets, Cases COMP/C-3/37.792 (Microsoft, 2004) to AT.40716 (App Store, 2024).

European Commission. Decisions designating gatekeepers under Article 3 of Regulation (EU) 2022/1925 (DMA): Alphabet, Apple, Meta, Amazon, Microsoft, and ByteDance. September 5, 2023.

European Commission. Decisions designating Very Large Online Platforms under Regulation (EU) 2022/2065 (DSA): Google, Amazon Store, Apple, Meta, Microsoft, Twitter, TikTok, Booking, and Wikimedia. April 25, 2023.

European Parliament. “Digital Markets Act: Application Timeline.” At a Glance: Digital Issues in Focus, November 30, 2022.

European Union (Withdrawal) Act 2018, s. 2(1) (UK).

Eurostat. “ICT Sector — Value Added, Employment and R&D.” Statistics Explained, April 2025.

Fella, Stefano, Leigh Gibson, Elena Ares, Claire Mills, Ilze Jozepa, Alistair Dillon, and Dominic Webb. “The UK-EU Reset: Next Steps after the May 2025 Summit.” House of Commons Library, July 29, 2025.

High-Level Expert Group on Artificial Intelligence (AI HLEG). “Ethics Guidelines for Trustworthy AI.” European Commission, April 8, 2019.

House of Lords, European Affairs Committee. Letter to Rt Hon Peter Kyle MP, Secretary of State for Science, Innovation and Technology. October 22, 2024.

Insee. Les comptes de la Nation en 2025. No. 2105, May 29, 2026.

Jordan, Jim. “Letter to EU Commissioner Teresa Ribera.” February 23, 2025.

Kon, G., et al. “The Data (Use and Access) Act 2025: Highlights of a Modest Reform to the UK’s Data Protection Laws.” Linklaters, 2025.

Labour Party. Manifesto 2024: Change. June 13, 2024.

Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l’espace numérique, JO May 22, 2024, art. 51 (France).

Malik, M. “Changement de régime: le discours intégral de J.D. Vance à Munich.” Le Grand Continent, February 14, 2025.

Marchant, N. “The Strange Rebirth of Singapore-on-Thames.” UK in a Changing Europe, January 14, 2025.

Memorandum of February 21, 2025: Defending American Companies and Innovators from Overseas Extortion and Unfair Fines and Penalties. 90 FR 10685. Federal Register, February 26, 2025.

Ofcom. “Important Dates for Online Safety Compliance.” October 16, 2024.

Office for Budget Responsibility. “Brexit Analysis.” March 2025.

Office for National Statistics. GDP Quarterly National Accounts, UK: October to December 2025. March 31, 2026.

Online Safety Act 2023 (Category 1, Category 2A, and Category 2B Threshold Conditions) Regulations 2025 (UK).

Online Safety Act 2023 (UK).

Pailler, Ludovic. “La protection des données à caractère personnel dans le marché européen des données.” RTD Eur., no. 3 (2025): 365–376.

Phillips, Merry. “Brexit: Could ‘Singapore-on-Thames’ Become Reality?” Per Incuriam, n.d.

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). May 4, 2016.
- Regulation (EU) 2022/1925 of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act). September 14, 2022.
- Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act). OJ L, October 19, 2022.
- Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act).
- Roda, J.-C. *Droit de la concurrence*. 2nd ed. Paris: Dalloz, 2025.
- Roland, Joël. *UK-EU Regulatory Divergence Tracker, Q4 2024–Q2 2025*. UK in a Changing Europe, July 16, 2025.
- Rough, E. “AI Regulation in the UK.” House of Commons Library, 2026.
- S.R. and T.B. “UK Watchdog Stops Short of Imposing EU-Style Rules on Apple and Google.” *Financial Times*, February 10, 2026.
- Snelson, S., F. Cilauro, F. Bruni, R. Woodhard, and D. Burton. *Data Flow and Economic Value EU Framework: Modelling Update and Data Collection*. Final Study Report. Luxembourg: Publications Office of the European Union, 2024.
- “Starmer Ready for Closer Alignment with the EU ’in the National Interest.’” *BBC News*, January 4, 2026.
- Turk, P. “Artificial Intelligence and Risks to Fundamental Freedoms.” No. 1 (2025): 28.
- UK Government. “New Strategy to Unleash the Transformational Power of Artificial Intelligence.” Press release, March 12, 2021.
- UK Government. “ONS UK Trade, Quarterly Trade in Goods and Services Tables: October to December 2025.” *Trade and Investment Core Statistics Book*. Accessed June 4, 2026.
- UK Government. “Trade Specialised Committee on Services, Investment and Digital Trade: Meeting 24 October 2024 — Minutes.” April 24, 2024.
- “UK-EU Alignment and Divergence: The Road Ahead.” *UK in a Changing Europe*, February 24, 2026.
- Untersinger, Martin, and William Audureau. “Quelle a été l’importance réelle de Cambridge Analytica dans la campagne de Trump?” *Le Monde*, March 21, 2018.
- Vidgen, B., H. Margetts, and A. Harris. “How Much Online Abuse Is There?” *The Alan Turing Institute*, 2019.
- Warman, Matt. “Written Statement: Data Protection and Digital Information.” UIN HCWS210. UK Parliament, July 18, 2022.
- Zogheib, Jean-Marc. “Effet de réseau.” *Dictionnaire de droit de la concurrence*. *Concurrences*, Art. No. 12231.

© GTPO 2026. All rights reserved. Short extracts may be quoted without express permission, provided the source is acknowledged. The opinions expressed in this publication are those of the author and do not necessarily reflect the institutional position of the Global Trade Policy Observatory, its team or its partners.