The global reach of the EU's approach to digital transformation

SUMMARY

The EU's approach to digital transformation is rooted in protecting fundamental rights, sustainability, ethics and fairness. With this human-centric vision of the digital economy and society, the EU seeks to empower citizens and businesses, regardless of their size. In the EU's view, the internet should remain open, fair, inclusive and focused on people. Digital technologies should work for citizens and help them to engage in society. Companies should be able to compete on equal terms, and consumers should be confident that their rights are respected.

The European Commission has published a number of strategies and action plans recently that outline the EU's vision for the digital future and set concrete targets for achieving it. The Commission has also proposed several digital regulations, including the artificial intelligence act, the Digital Services Act and the Digital Markets Act. These regulations are intended to ensure a safe online environment and fair and open digital markets, strengthen Europe's competitiveness, improve algorithmic transparency and give citizens better control over how they share their personal data.

Although some of these regulations have not yet been adopted, and others have been in force for only a short time, they are expected to have impact not only in the EU but also beyond its borders. For instance, several regulations target businesses – regardless of where they are based – that offer services to EU citizens or businesses. In addition, through the phenomenon known as 'the Brussels effect', these rules may influence tech business practices and national legislation around the world.

The EU is an active participant in developing global digital cooperation and global governance frameworks for specific areas. Various international organisations are developing instruments to ensure that people and businesses can take advantage of artificial intelligence’s benefits and limit negative consequences. In these global negotiations, the EU promotes respect for various fundamental rights and freedoms, as well as compatibility with EU law.
Introduction

The EU is increasingly aware that although digital technologies can enrich our lives in many ways, they also come with a number of challenges, such as cyber-attacks, the digital divide, the spread of disinformation, and the concentration of power in a handful of tech companies. According to the European Commission, ‘Europe must now strengthen its digital sovereignty and set standards, rather than following those of others – with a clear focus on data, technology, and infrastructure’.

The Council conclusions on EU digital diplomacy, published in July 2022, set a number of objectives for the EU. These include influencing international technology standards by promoting ethical, safe and inclusive standards, and helping to develop resilient and trusted digital infrastructures beyond its borders (via its Global Gateway strategy).1

In recent years, the Commission has proposed a cascade of non-legislative and legislative acts in the domain of digital transformation, to keep pace with developments in digital technologies. Analysts have referred to this as ‘policy and regulatory activism’. Recent acts include the Digital Services Act (DSA), the Digital Markets Act (DMA), the artificial intelligence act (not yet adopted), the Chips Act, the Data Governance Act, the Data Act, the Cybersecurity Act and the cyber resilience act (not yet adopted). Following in the footsteps of the General Data Protection Regulation (GDPR), several of these digital regulations seek to ensure a safe online environment and fair and open digital markets, strengthen Europe’s competitiveness, improve algorithmic transparency and give citizens better control of how they share their personal data.

Improving competitiveness is particularly important, as the EU does not currently hold the strongest position in the global ICT market. According to the 2023 digital decade report and the CERRE 2022 report on digital industrial policy for Europe, the EU relies on foreign countries for over 80% of digital products, services, infrastructures and intellectual property.

Although some of these digital regulations (such as the AI act) have not yet been adopted, and others have been in force for only a short time (for example, the DSA and the DMA), analysts expect them to have an impact not only within the EU, but also beyond its borders. Several digital regulations affect companies that offer services to EU citizens or businesses, regardless of whether or not the company is based in the EU (see later sections on the DSA and DMA). Some scholars, such as Anu Bradford, believe that the recent EU digital regulations will influence global tech business practices and other countries’ legislation via a phenomenon called the Brussels effect (see box). Namely, tech companies may choose to extend EU rules across their global business operations in an effort to standardise their products and services. Furthermore, governments of other countries may take inspiration from the EU’s digital regulations (see later sections).

The Brussels effect

The ‘Brussels effect’ is a term introduced by Columbia Law School professor Anu Bradford. It refers to the EU’s ‘unilateral power to regulate global matters’. There are two key ways in which EU rules may be exported: the de facto Brussels effect and the de jure Brussels effect.

The de facto Brussels effect occurs when companies voluntarily extend EU rules across their global businesses. The EU is one of the world’s largest and wealthiest markets. Most global companies wish to trade in the EU. However, the price for accessing this market is adjusting their conduct and production to meet some of the globe’s most stringent standards. Rather than bear the cost of running separate compliance regimes, companies might apply the EU rules to their operations beyond the EU. (This only applies if the benefits of adhering to a single standard outweigh the benefits of taking advantage of laxer standards elsewhere).

With the de jure Brussels effect, foreign governments adopt EU-style regulations. This might happen, for example, as a result of lobbying by companies that have extended the EU rules across their global businesses, or as a result of the EU’s political influence.

The EU cooperates with many countries to represent EU interests, values and norms related to the digital transformation. With certain countries, this partnership is regular and structured, while with others, consists solely of high-level dialogues. For example, the EU has launched trade and technology councils with the United States and India, which meet regularly at the ministerial as well as working group level. With countries such as Canada, Japan, Korea and Singapore, the EU has built digital partnerships in the form of annual ministerial meetings, workshops for specialists and sectoral dialogues. The EU has launched a cyber-dialogue with Ukraine to help the country counter cyber-attacks. The EU also holds high-level dialogues with countries with which it does not necessarily share all values. For example, the EU has held high-level digital dialogues with China. Through these cooperative efforts, the EU and its partners share information, gain better understanding of existing legislation of the other party, define best practices, identify risks and explore options for closer cooperation in areas such as artificial intelligence (AI), global connectivity, safety of online products and data regulation. With some countries, the EU has defined common action plans (such as the US-EU joint AI roadmap and the EU-China action plan on the safety of products sold online). The EU is working with the United States to develop common terminology (see box 'Collaboration with the United States on shared AI terminology').

Furthermore, the EU seeks to promote its approach to digital transformation through agreements made in international organisations and multilateral fora. It works with the OECD, the G7, the G20, the Council of Europe, the United Nations (UN) and many other organisations. For example, the EU is participating in developing a global vision for digital cooperation through the United Nations' Global Digital Compact initiative. The initiative aims to outline a shared vision of how countries all over the world could cooperate to deal with issues such as the digital divide, disinformation, cyber threats and risks posed by AI. As highlighted by Josep Borrell, the High Representative of the European Union for Foreign Affairs and Security, the EU has stressed in these negotiations that the digital transformation should serve people, not big tech companies or state interests.

Various international organisations (including the Council of Europe) are currently developing global governance frameworks for specific areas like AI (see section on global governance and collaboration framework for AI). In these initiatives, the EU is promoting the respect of various fundamental rights and freedoms as well as compatibility with EU law and the future AI act.

The EU's vision for the digital transformation

As evidenced in a number of high-level statements and declarations, the EU has put the digital transformation high on its agenda. Building 'a Europe fit for the digital age' is one of the six European Commission priorities for 2019-2014. Commission President Ursula von der Leyen's political guidelines for the Commission in 2019-2024 stress that Europe needs to achieve sovereignty in key technological areas. It must also set standards for these technologies that will ideally become the global norm. The Commission President believes that Europe has already taken significant steps in this direction and has become a pioneer in citizens' rights in the digital world.

In 2021, the Commission declared the period from 2020 to 2030 Europe's 'digital decade'. It set specific targets for 2030 for digital skills, digital infrastructures, and digitalisation of businesses and public services. One of the key challenges in this period is securing the EU's technological and digital sovereignty. For this reason, the EU has sought to boost investments in critical technologies such as semiconductors, supercomputing and 6G (through the Chips Act, the European high-performance computing joint undertaking, and the Hexa-X project, respectively, to give just a few examples). Supporting the digital transition is key part of the EU's post-pandemic economic and societal recovery efforts. Namely, EU Member States have to earmark at least 20% of the resources of their national recovery and resilience plans for achieving digital targets.

The EU’s digital agenda is deeply rooted in the protection of fundamental rights, democracy and fairness. This is reflected, for example, in Article 2 of the Treaty on European Union: ‘(T)he Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law
and respect for human rights, including the rights of persons belonging to minorities’. The charter of fundamental rights of the EU further strengthens these values by protecting specific rights and freedoms, such as the rights to private life, protection of personal data, freedom of expression, non-discrimination, consumer protection and freedom to conduct a business. These rights and freedoms are cited in many digital policy initiatives. For example, the Data Act refers several times to fundamental rights, in particular the right to protection of personal data.

As stated in several Commission documents (such as the 2021 communication announcing the digital decade and the 2020 communication outlining the EU’s vision of the digital future), the EU seeks to promote a human-centric vision of the digital economy and society that empowers people. Both communications also highlight the EU’s aim to shape global and bilateral rules for digital trade along European values. In the EU’s view, technology should work for people and help them to engage in society. Companies should be able to compete on equal terms, and consumers should be confident that their rights are respected. The internet should remain open, fair, inclusive and human-centric. The digital transformation should contribute to a sustainable, climate-neutral and resource-efficient economy. The EU promotes ethical rules, which increase trust in digital technologies.

The EU outlined similar principles in the declaration on European digital rights and principles, jointly adopted in 2022 by the European Parliament, the Council and the Commission. According to the declaration, the digital transformation should benefit everyone and improve ‘the lives of all people living in the EU’. The declaration emphasises citizens’ rights, fair competition, inclusiveness and sustainability. As stated in the declaration, people should be able to make their own informed decisions regarding digital technologies and be able to choose which online services they use. They should be safe from illegal and harmful content and be empowered when interacting with new technologies such as AI. Their privacy and personal data should be protected, and their working conditions should be fair. The declaration also highlights the need to protect children and young people, while empowering them to make safe and informed choices in the online environment. Furthermore, it stresses the importance of trust, diversity and multilingualism in the digital world.

Promoting the EU's vision at a global level

The artificial intelligence act as a global standard

In April 2021, the European Commission proposed a piece of horizontal legislation on artificial intelligence (the ‘AI act’) that aims to create harmonised rules for AI systems sold and used in all 27 EU Member States. On 9 December 2023, the European Parliament and the Council reached a provisional agreement on this act. The draft AI act is the first ever attempt to enact a horizontal regulation on AI. With this regulation, the EU aims to give users confidence in AI-based solutions, and encourage businesses to develop them. In addition, the EU is working on an AI liability directive, which aims to protect victims of AI misuse or damage.

The AI act proposes a risk-based approach to AI systems. AI systems are sorted into categories based on the level of risk they pose: high risk, limited risk or minimal risk. The act specifies which applications of AI fall into each category. It also proposes to prohibit certain AI applications that pose risks to health, safety, or fundamental rights deemed unacceptable (for example, AI systems that exploit vulnerable persons or groups). ‘High-risk’ AI systems would be authorised, but subject to a set of requirements and obligations, whereas AI systems presenting only ‘limited risk’ would be subject to very light transparency obligations.

In the provisional agreement, the co-legislators have banned additional AI applications (such as social scoring based on personal traits or characteristics) and added that deployers of high-risk AI systems will have to carry out a fundamental rights impact assessment. The provisional agreement also includes rules on general-purpose AI models (including foundation models) that can be adapted to various tasks (such as ChatGPT). Providers of AI systems, including general-purpose AI
The global reach of EU’s vision to digital transformation

systems, will have to disclose when content is generated by AI and not by humans. High-risk general-purpose AI systems will be subject to stricter obligations, such as the obligations to assess and mitigate systemic risks, conduct adversarial testing and report serious incidents to the market surveillance authority of the Member State where the incident occurred.

The AI act has been designed to have worldwide effects and support the EU in becoming ‘a global leader in the development of secure, trustworthy and ethical artificial intelligence’. The AI act also seeks to strengthen the EU’s digital sovereignty. As highlighted in the impact assessment accompanying the Commission proposal, there is a danger that if the EU does not adopt a common framework for AI technology, diverging national approaches could lead to market fragmentation, creating obstacles for businesses (in particular, for small and medium-sized enterprises). This in turn could negatively affect the global competitiveness of EU businesses that provide and use AI systems, giving an advantage to companies from third countries.

The EU does not currently hold the strongest position in the global AI market. As seen in Figure 1, the EU has far fewer AI players than China or the United States. The EU also invests less in AI than other economies. According to a Joint Research Centre 2022 report on AI investment in the EU, the United States spends nearly twice as much as the EU on AI research and development and AI-related complementary assets.

Since the AI act is not yet in force, it is difficult to predict whether the EU will achieve its goal of becoming a global leader in AI development. Some analysts argue that the AI act will not necessarily help European AI players become more innovative or plentiful. However, they posit, the likelihood is high that new regulation will protect fundamental rights and promote European values and principles as AI develops.

The AI act may also influence the global practices of AI developers. In her book, ‘Digital Empires’, Anu Bradford explains why AI developers might be motivated to apply AI act rules to other markets. Namely, if AI developers wanted to expand into the EU market, or include European data when training their algorithms, they would have to comply with AI act requirements. If these developers offered the same AI applications to non-EU markets, they would also have to train their algorithms on different, non-EU data. Because such a division may not be economically favourable, developers may instead decide to simply apply the EU rules to all markets, in order to be able to use EU data while minimising costs. Additionally, it could be difficult for AI developers to explain why they have to disclose when content is generated by AI in the EU market, but not in other markets.

Other analysts argue that the Brussels effect of the AI act might be more limited. As Alex Engler notes in his recent article, the EU is not alone in setting standards for AI. Other big markets, such as China, are working on their own regulations. In addition, several international organisations and bodies are working on a global governance framework for AI. As well as inspiring other bodies, the EU at times draws from the work of others, as it did when developing a definition of AI systems.

Global collaboration and governance framework for AI

The EU is working with partners to develop a range of global AI governance and collaboration instruments to enable users to reap AI’s benefits while avoiding negative consequences. A number of international organisations have launched initiatives in which they outline general values and principles regarding AI. In these negotiations, the EU advocates for respect of fundamental rights and freedoms as well as compatibility with EU law and the AI act.
Some of these initiatives aim to be legally binding. For example, the Council of Europe’s Committee on AI is developing a legally binding international instrument on AI, human rights, democracy and the rule of law (the ‘convention on AI’). The convention would be open to countries that are not members of the Council of Europe. The draft version of the convention, published in December 2023 (yet to be adopted) has a number of similarities with the Commission’s proposal for an AI act (as well as with the provisional agreement on the AI act). Both texts follow a risk-based approach to regulating AI systems and put emphasis on the respect of fundamental rights and freedoms (such as the rights to human dignity, privacy and personal data protection). However, unlike the AI act, the convention on AI combines this risk-based approach with principle-based elements that apply to all AI applications within its scope. The AI act is also much more detailed than the convention on AI.

The exact scope of the convention on AI is still being discussed. Namely, the draft version of the convention includes a possibility of leaving the private sector out of its scope. According to media, the European Commission is against this limitation.

Other global initiatives simply give guidance or recommendations on AI related issues. For example, in November 2021, the 193 Member States of the United Nations signed UNESCO’s first-ever global standard on AI ethics – the ‘recommendation on the ethics of AI’. This document gives guidance on how to ensure that AI is developed and used ethically. The UNESCO recommendation outlines a number of values and principles (such as transparency, safety and security, non-discrimination, privacy, sustainability and inclusion) that should be respected by all actors across the AI system lifecycle. It warns against dangerous uses that threaten civil rights – for example, using AI systems for social scoring or mass surveillance. However, since the recommendation is not legally binding, these principles are not always respected by its signatories. For example, China uses AI for social scoring and mass surveillance, despite having signed the UNESCO recommendation.

The intergovernmental political forums G7 and G20 have adopted their own AI principles, both of which have been signed by the EU. The G7 and G20 stress respect for rule of law, human rights and democratic values such as diversity, fairness, democracy and privacy. The G20 AI principles, adopted in June 2019, calls on AI actors to be fair, transparent and accountable throughout the AI system lifecycle. In the G7 guiding principles on AI (accompanied by a code of conduct for AI developers), adopted in October 2023, organisations that design, develop, deploy and use AI systems are urged to identify, evaluate and mitigate risks and vulnerabilities across the AI lifecycle and make it easy for users to report issues. The G7 supports a risk-based approach and measures that enable users to better identify AI-generated content. In addition, the G7 countries call for the prioritization of research that helps to improve AI safety and security and pays special attention to personal data and intellectual property protection.
Both the G7 and G20 AI principles build on the OECD recommendation on AI, adopted in May 2019. The OECD recommendation, developed by the OECD Council on Artificial Intelligence, proposed several AI-related definitions, including a definition of an AI system. The OECD subsequently modified this definition to reflect the latest scientific consensus on AI systems. The definition now reads as follows: ‘An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment’. As proposed by the European Parliament, the EU is considering using a similar definition in the EU AI act. Similarly to the AI act, the OECD recommendation promotes a number of human-centred and democratic values, such as human dignity, privacy, personal data protection, equality and non-discrimination.

The EU has also signed international declarations that boost cooperation in the field of AI. At the AI Safety Summit, held on 1 and 2 November 2023 at Bletchley Park (United Kingdom), the EU, together with 28 countries from across the globe (including Australia, China, India, the United Kingdom and the United States) signed the Bletchley Declaration, which aims to boost global cooperation on increasing AI safety. The declaration encourages governments, companies, civil society and academia to cooperate to ensure safety of AI. In particular, it proposes two objectives: 1) identifying AI safety risks of shared concern and 2) developing AI policies that follow a risk-based approach in all countries that signed the declaration.

The Digital Services Act as a global standard

The EU may also use the Digital Service Act (DSA), adopted in November 2022, to promote its vision of digital transformation and influence global tech companies’ practices. The DSA lays out rules regarding the responsibilities of different types of online intermediary services that provide consumers with goods, services and content, online platforms, very large online platforms (VLOPs) and very large online search engines (VLOSEs).

The DSA obliges online platforms and online search engines to combat harmful and illegal content as well as the sale of illegal goods and services. They must put measures in place that make reporting illegal content, goods or services easy for users and delete illegal content promptly. Furthermore, such online platforms have to publish information detailing how they moderate content (including the number of removal orders and their automatic content moderation tools). In addition, the DSA imposes certain limits on the presentation of advertising and on the use of sensitive personal data (such as sexual orientation, religion and ethnicity) for targeted advertising. Targeted advertising based on minors’ personal data is prohibited. VLOPs and VLOSEs will have to comply with stricter annual risk assessments and external auditing obligations, and share data with researchers and authorities on content moderation decisions. The DSA also imposes significant financial penalties on infringing companies, which could be fined up to 6% of their total worldwide annual turnover. In April 2023, the European Commission designated a first set of VLOPs and VLOSEs and in December 2023, the second set of VLOPs. (These nominations are being challenged in the European Court of Justice by some of the identified companies, including Amazon and Zalando).

The European Commission has already taken investigatory steps into several companies to assess their compliance with the obligations set by the DSA. In October 2023, the Commission sent information requests to X (formerly Twitter), Meta, TikTok and Aliexpress to check if they abide by DSA rules regarding the fight against illegal content, disinformation (for example, as regards the Israeli-Hamas conflict) and illegal products (such as fake medicines).

The DSA rules can extend beyond the EU in several ways. First, the DSA applies to providers of intermediary services irrespective of their place of establishment or residence, if they provide services in the EU (Article 2 of the DSA). Therefore, it applies to non-EU companies. Furthermore, companies may decide to apply DSA rules to services offered to third-country citizens and businesses, if it is in the company’s interests to do so. For example, it might be difficult for an online
Platform to explain to customers why, in the EU, users can influence and modify the content they see, while users in other markets cannot. Similarly, it could be difficult to explain why minors using their services in the EU are protected from targeted advertising, but not minors living elsewhere.

Parallels can also be found between the DSA and legislation from other countries – for example, the UK’s Online Safety Act, adopted in October 2023. Both the DSA and the Online Safety Act strive to balance content moderation with protecting freedom of speech. Both introduce obligations for companies to address harmful and illegal online content and activities. Although the two acts do not apply to the exact same services,14 both include reporting requirements, risk assessments, and procedural rights of appeal. Both acts also impose penalties on infringing companies (up to 10 % of a provider’s worldwide qualifying revenue – and even imprisonment – in the Online Safety Act). The main difference is that the Online Safety Act is less specific than the DSA, requiring telecommunications regulator Ofcom to provide more detailed codes of conduct.

The Digital Markets Act as a global standard

Another recent digital regulation with potential global impact is the Digital Markets Act (DMA), adopted in September 2022. The DMA seeks to ensure contestable and fair markets when digital platforms that act as ‘gatekeepers’ are present. According to the DMA, a provider of core platform services (CPS) ‘shall be designated as a gatekeeper if: a) it has a significant impact on the internal market; (b) it provides a CPS that is an important gateway for business users to reach end users; and (c) it enjoys an entrenched and durable position in its operations or it could enjoy such a position in the near future’. The DMA sets quantitative thresholds for a company to fall within its scope, such as having €7.5 billion in annual turnover or having at least 45 million monthly active end users and at least 10 000 active business users. In September 2023, the Commission designated six gatekeepers under the DMA: Alphabet, Amazon, Apple, ByteDance, Meta and Microsoft. Some of these companies have sought DMA exemption for some of their CPSs (for example Microsoft for its Bing, Edge and Microsoft Advertising services, and Apple for its iMessage service). The Commission is carrying out market investigations to review these contested gatekeeper designations.

The DMA sets a number of dos and don’ts for gatekeepers. For example, gatekeepers have to allow users to easily uninstall pre-installed apps and change default settings. They must also allow business users to advertise and conclude contracts with customers outside the gatekeeper’s platform. Gatekeepers may not rank their own products or services more favourably than those of third parties, or require app developers to use particular proprietary services (such as payment systems) in order to appear in their app stores. The DMA foresees financial penalties for infringing companies (up to 20 % of worldwide turnover for repeated offences) and structural remedies in cases of systematic non-compliance (e.g. a fixed-term ban on acquiring other companies).

Like the DSA, the DMA applies to companies, irrespective of their place of establishment or residence, that provide their CPSs to users established or located in the EU. The DMA also has similarities with legislative proposals from other countries, such as the UK’s pending Digital Markets, Competition and Consumers Bill, proposed on 25 April 2023 in the House of Commons. Both acts tackle the problem of market imbalances in the digital economy and lay down provisions designed to increase competition in digital markets and protect consumer rights. They both apply only to certain undertakings (called ‘gatekeepers’ in the DMA and ‘undertakings having strategic market status’ in the Digital Markets, Competition and Consumers Bill) but differ largely in the specific provisions. While the DMA lays down specific dos and don’ts for gatekeepers, the UK bill only provides a framework and objectives, leaving the UK Competition and Markets Authority to set specific rules. Unlike the DMA, the UK bill does not identify core platform services. While the DMA defines the size of companies that fall under its scope (in terms of active end users and business users), the UK bill does not define a jurisdictional threshold for users. It simply requires the presence of a ‘significant number of UK users’.
Conclusion

As described above, EU digital legislation is likely to have an impact that extends well beyond the EU's borders. The rules often apply to all companies – irrespective of their place of establishment or residence – providing their users are established or located in the EU. In addition, the EU is influencing the practices of global tech companies via a phenomenon referred to as the 'Brussels effect', whereby certain companies voluntarily extend EU rules across their global businesses.

In the EU's view, the digital transformation should serve people, not big tech companies or state interests. The EU is working to influence digital negotiations at the global level, to ensure that initiatives such as the Council of Europe’s convention on AI and the UN Global Digital Compact respect fundamental values and freedoms. Many of these negotiations are ongoing, and although still in the initial stages, similarities with EU legislation can be found. The extent to which the Brussels effect will take global hold remains to be seen.

The EU is also exploring ways to cooperate more closely with individual countries. In some cases, this cooperation has resulted in concrete results, such as action plans on how to ensure safety of products sold online. In other cases, high-level dialogues are taking place. There is much work ahead to ensure that citizens and businesses can take advantage of the possibilities offered by AI, without suffering negative consequences.

MAIN REFERENCES


ENDNOTES

1 The Global Gateway is an EU strategy that helps to boost smart, clean and secure links in the digital, energy and transport sectors and to strengthen health, education and research systems across the world.

2 E.g. strategies, action plans.

3 E.g. regulations, directives.

4 Not yet adopted.

5 Other countries (such as China) have proposed targeted AI regulations, addressing recommendation algorithms, generative AI, etc.

6 Providers of AI services and applications.

7 The Council of Europe is an organisation of 46 Member States (including all EU Member States) that promotes democracy, human rights and the rule of law in Europe and beyond.

8 The latter was tasked with developing a convention (or framework convention) on the development, design and application of AI based on the Council of Europe standards for human rights, democracy and the rule of law. The CAI builds upon previous work done in the Council of Europe, in particular that of the Ad Hoc Committee on AI (CAHAI), which, in the years 2019-2021, identified possible elements of a legal framework on AI.

9 Published in July 2023.

10 The G7 group consists of Canada, France, Germany, Italy, Japan, the United Kingdom and the United States. The EU takes part in discussions.

11 The G20 group comprises 19 states (Argentina, Australia, Brazil, Canada, China, France, Germany, India, Indonesia, Italy, Japan, the Republic of Korea, Mexico, Russia, Saudi Arabia, South Africa, Turkey, the United Kingdom and the United States) and two regional bodies: the European Union and the African Union.

12 In the initial OECD recommendation, the organisation defined an AI system as follows: ‘an AI system is a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy’.

13 The Parliament proposed the following wording: ‘AI system means ‘a machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions, that influence physical or virtual environments’.

14 The DSA applies to various types of intermediary services. The Online Safety Act applies to search services and user-to-user services that allow individuals to share content online.

DISCLAIMER AND COPYRIGHT

This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament.

Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy.

© European Union, 2024.

Photo credits: © sodawhiskey / Adobe Stock.
eprs@ep.europa.eu (contact)
www.eprs.europa.eu (intranet)
www.europarl.europa.eu/thinktank (internet)
http://epthinktank.eu (blog)