UNIVERSITÄT BONN

ZEI Center for European Integration Studies

Future of Europe Observer

Vol. 10 No. 3 October 2022

The digital transformation is one of the most important developments of the recent past. In order to keep pace with this and to actively shape and steer it, the EU has made digital legislation one of the most important issues. This issue takes a closer look at the legislation in the area of digitalisation and deals with the major projects and recent developments. In particular, the Digital Markets Act and the Digital Service Act are the European Union's flagship legislation packages, which is why they are examined in detail. It also looks at developments in digital infrastructure, digital healthcare and the space programme.

Contents

Future of Europe Observer

accompanies the debate on governance and regulation in the European Union. Authors are ZEI Scholars, Master of European Studies Fellows, and Alumni.

The European digitalisation ambition: Halfway there?

"Digital transition is accelerating", proclaimed Margrethe Vestager recently, Vice-President of the Commission in charge of "A Europe for the Digital Age". She made this statement when presenting the results of the Digital Economy and Society Index (DESI) at the end of July 2022. The report noted clear progress in the area of digital expansion, even if there were still glaring gaps. The DESI is a first interim report on the Commission's digitalisation ambitions, which took on a very concrete form last year with the Digital Compass. By 2030, very specific goals are to be implemented, the digital transformation in companies and the public sector is to be driven forward, and skills and a secure and sustainable infrastructure are to be created (Commission 2021).

In addition to the transition of the European economy in the course of the Green Deal to a sustainable eco-social economy, the digital transformation is the second major project of the Von der Leyen Commission. Therefore, in retrospect, its success will also be measured decisively by the progress made in this area. It is crucial for the future of the EU that the issues of digital sovereignty, cyber security, key technologies, cloud computing and digital infrastructure are not only addressed, but that the EU is enabled to take a leading role in these areas. Only through structural change will the European Union be able to thrive economically and socially and solve the problems of the future.

Half of the current Commission's legislative period is now over, which raises the question whether half of the intended goals have been achieved. In this regard, the Digital Economy and Society Index (DESI) states that the expansion of infrastructure in the form of fibre-optic expansion is progressing and individual Member States in particular, such as Italy, Poland and Greece, have made great progress in the area of digitalisation in recent years. All three have placed a greater political focus on this topic area and made sustainable investments. However, there are still huge deficits in the use of key technologies such as AI and big data by companies, which remains extremely low across the EU at 8 per cent and 14 per cent respectively. Especially in light of the fact that the usage target is 75 per cent by 2030. Furthermore, it is particularly striking that only 54 per cent of Europeans between the ages of 16 and 74 have at least basic digital skills. Furthermore, there continues to be a massive skills shortage in ICT, as the EU is far behind the 20 million target with only 9 million ICT specialists to date. This shortage is a major obstacle to business competitiveness and the implementation of digital transformation in the EU (DESI 2022).

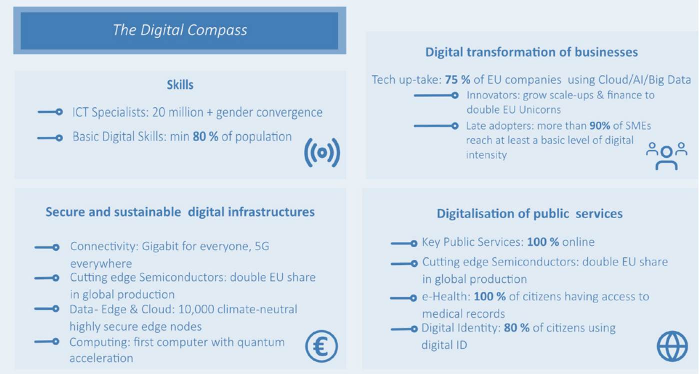
In view of this, the speed of digitalisation must once again increase significantly if the EU targets are to be achieved. The digital transformation remains an ambitious project, which is being shaped by several future and past legislative projects in the last two years. Whereby many legislative acts have yet to be implemented or have yet to have an impact. How consistent the EU is in implementing its policy goals and how effective its measures are, must be monitored and is highlighted in this issue of the Future of Europe Observer.

Henrik Suder, *Research Fellow at ZEI, University of Bonn.*

Overview of the EU's digitisation goals

Ever since assuming the position as the President of the European Commission in 2019, Ursula von der Leyen has been encouraging a Union-wide approach that allows EU's citizens as well as its businesses to effectively adjust to the digital transformation. Strengthening digital sovereignty and working according to standards that adequately reflect European norms and values shall essentially contribute to a climate-neutral Europe (European Commission 2019).

Issues that will be addressed in the upcoming years include the dependency on non-European technology, disinformation and its impact on democratic societies as well as the promotion of an economy that is climate neutral, circular and resilient. With the so-called Digital Compass, which plays a central part in EU's digital transformation, the terms and specific targets for the 2030 digital goals are defined. Apart from agreeing on a set of digital principles, launching multi-country projects and commencing a legislative proposal for a robust governance framework, there are several policies listed that require concrete action (European Commission 2021).



The Digital Compass

Skills

- ICT Specialists: 20 million + gender convergence
- Basic Digital Skills: min **80 %** of population

Digital transformation of businesses

Tech up-take: **75 %** of EU companies using Cloud/AI/Big Data

- Innovators: grow scale-ups & finance to double EU Unicorns
- Late adopters: more than **90%** of SMEs reach at least a basic level of digital intensity

Secure and sustainable digital infrastructures

- Connectivity: Gigabit for everyone, 5G everywhere
- Cutting edge Semiconductors: double EU share in global production
- Data- Edge & Cloud: 10,000 climate-neutral highly secure edge nodes
- Computing: first computer with quantum acceleration

Digitalisation of public services

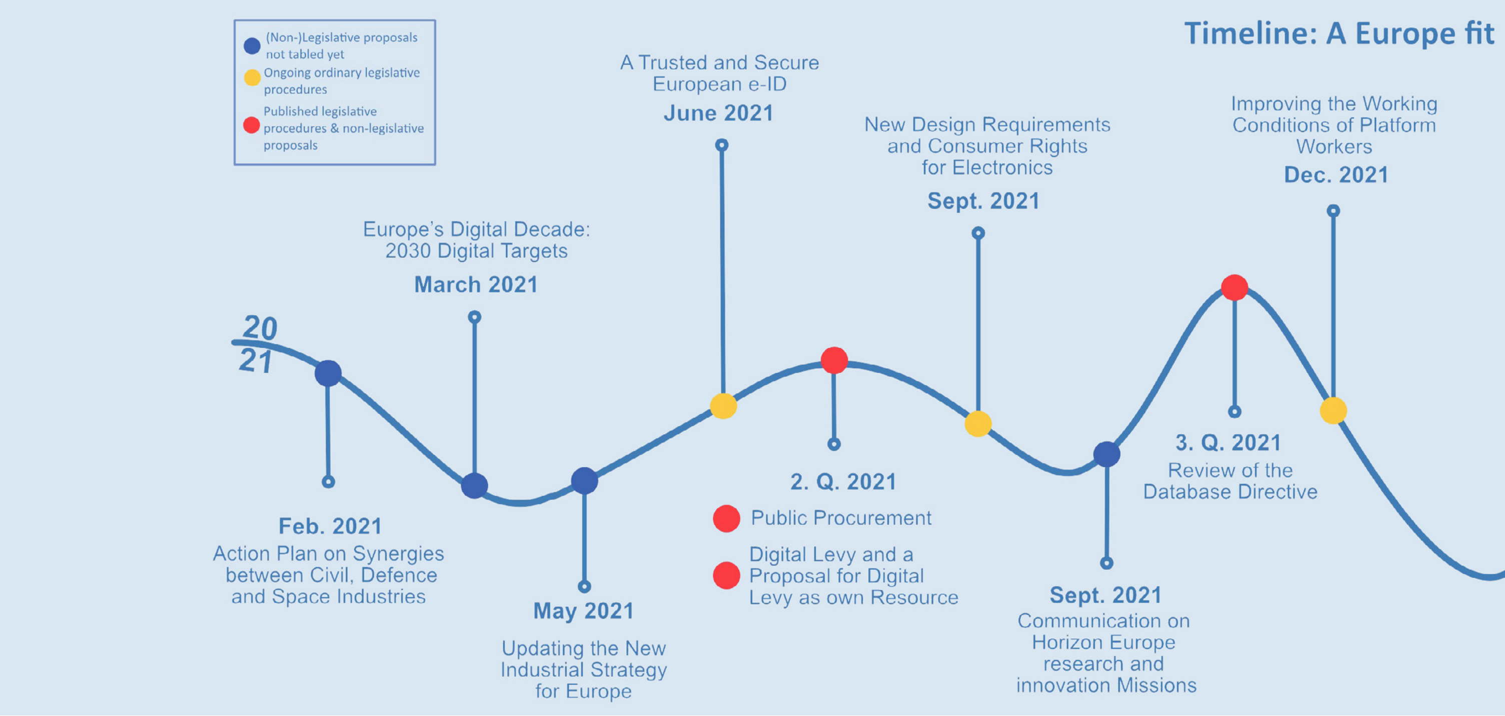
- Key Public Services: **100 %** online
- Cutting edge Semiconductors: double EU share in global production
- e-Health: **100 %** of citizens having access to medical records
- Digital Identity: **80 %** of citizens using digital ID

(European Commission 2021)

Further action necessary for building Europe's digital transition in critical areas will address multi-country projects, relying on investments from the EU-budget, member states, industry, the Recovery and Resilience Facility and other EU funding. Possible project ideas include a pan-European interconnected data processing infrastructure and the deployment of the next generation of low power trusted processors (European Commission 2021).

Taking into consideration the rapid increase in social media usage among EU's citizens, a framework for digital principles (e.g. access to high quality connectivity, to sufficient digital skills, to public services) will ensure that the same rights that apply offline can be fully exercised online. An annual Eurobarometer will assess whether Europeans feel their rights adequately protected (European Commission, Presscorner 2021). Lastly, complementing the priority "A Stronger Europe in the World", the EU aspires to promote its digital standards within international organisations, primarily through international partnerships. The aim is to exert common global objectives for common global challenges (European Commission n.d.).

Mara Nazaretyan, *ZEI Student Assistant, Uni Bonn.*


Timeline: A Europe fit
● (Non-)Legislative proposals not tabled yet
● Ongoing ordinary legislative procedures
● Published legislative procedures & non-legislative proposals
20
21
Feb. 2021
Action Plan on Synergies between Civil, Defence and Space Industries
Europe's Digital Decade: 2030 Digital Targets
March 2021
May 2021
Updating the New Industrial Strategy for Europe
A Trusted and Secure European e-ID
June 2021
2. Q. 2021
Public Procurement
Digital Levy and a Proposal for Digital Levy as own Resource
New Design Requirements and Consumer Rights for Electronics
Sept. 2021
Sept. 2021
Communication on Horizon Europe research and innovation Missions
3. Q. 2021
Review of the Database Directive
Improving the Working Conditions of Platform Workers
Dec. 2021

The EU-Digital Acts or an upcoming “digital regulation”

From GDPR to DGA, DA and DSA, from DMA to AI: these are abbreviations that only mean something to the insiders. They stand for new legal acts from Brussels, which as Regulations are supposed to directly, immediately order the new digital world in the EU Member States. Some of these Regulations have been in force for some time now or recently, while others are currently going through the legislative process. All of them are interrelated. They have different objectives but are not clearly demarcated from one another and have to be applied in parallel in parts. The digital regulatory efforts from the EU are now so comprehensive and diverse that creating an overall view poses challenges, which this Article at hand addresses. The aim of the following analysis is to systematise the current efforts of digital regulation from the EU and to place them in a plausible context.

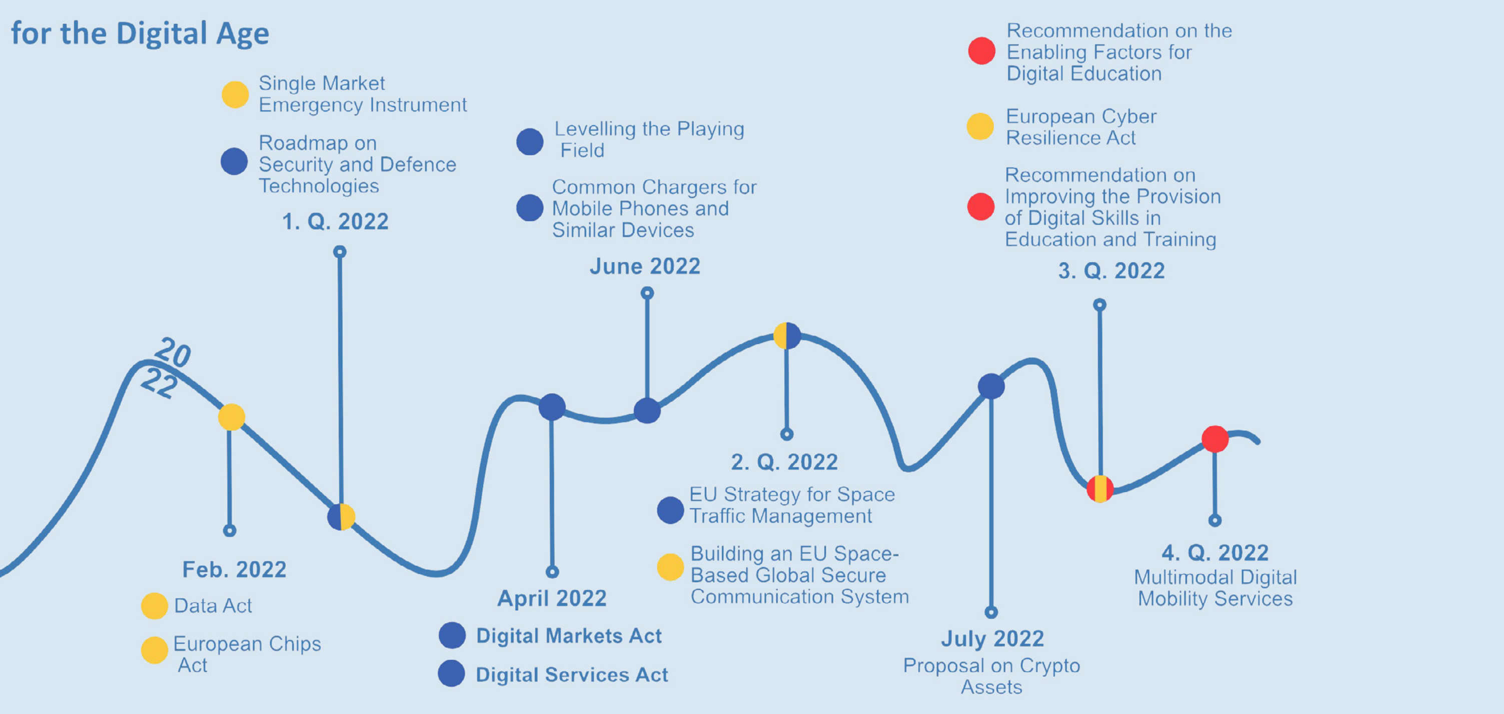
Introduction: The digital strategy

Digital products and services have become an indispensable part of our everyday lives. Meetings are held via video conferencing, presentations are edited together with colleagues in the cloud and by using collaborative tools, and complex software solutions analyse empirical findings. Our private lives are also based on digital applications, from smart TVs and eBook readers to quick exchanges with friends via messenger and social media platforms.

However, does this digital world have its own law? So far, the EU legislator has mostly endeavoured to regulate in a technology-neutral and development-open manner. In sector-specific regulation of the telecommunications market, for example, this has been a cherished principle for years. This approach is important because it leaves the market free to innovate and prevents legislators from always being “too late” and lagging behind actual developments.

Nevertheless, the EU has been pursuing a more specific approach for some years now: In February 2020, the European Commission published the EU’s Digital Strategy (COM(2020) 67 final) to shape Europe´s digital future. The actions presented in the strategy aim to achieve a value-based digital transformation that will work for all, put people first and open new opportunities for businesses (COM(2020) 67 final, p. 1 et seq.). Social development shall be achieved as well as a sustainable use of digital technologies, taking into account the fundamental rights and freedoms of all those involved in private as well as business. Digital competence, a vivid data economy and data fairness are core goals.

The strategy and its actions also include the enactment of a large number of new legal acts that are intended to regulate the most diverse areas of the digital world, each of which pursues different objectives whereby there are partly criticised overlaps. More or less 50 legal acts can be assigned to this strategy (Schmitz ZD 2022, 189).


for the Digital Age
20
22
Single Market Emergency Instrument
Roadmap on Security and Defence Technologies
1. Q. 2022
Feb. 2022
Data Act
European Chips Act
Levelling the Playing Field
Common Chargers for Mobile Phones and Similar Devices
June 2022
April 2022
Digital Markets Act
Digital Services Act
2. Q. 2022
EU Strategy for Space Traffic Management
Building an EU Space-Based Global Secure Communication System
Recommendation on the Enabling Factors for Digital Education
European Cyber Resilience Act
Recommendation on Improving the Provision of Digital Skills in Education and Training
3. Q. 2022
July 2022
Proposal on Crypto Assets
4. Q. 2022
Multimodal Digital Mobility Services

(European Union 2022)

The EU-Digital Acts or an upcoming “digital regulation”

These legal acts for the regulation of the digital world have been appearing for several months now as if on an assembly line. Keeping track of them is a challenge. This article puts the most important new and upcoming legal acts into the overall context. What is being created here is a new digital regulation - or in other words, a new regulation of the digital world.

What has happened in recent years

More than 4 years ago, Regulation (EU) No. 2016/679, the GDPR, came into force as a comprehensive regulation for the processing of personal data. The GDPR was as a kind of starting signal for digital regulation from Brussels (even if, strictly speaking, the GDPR also applies to analogue, non-automated data processing as long as it is systematic). The GDPR was supposed to be accompanied by the ePrivacy Regulation, which, in parallel to the GDPR, regulates special aspects of the handling of electronic communications, telemedia and the integrity of the end devices of us users. The ePrivacy Regulation has not yet been adopted, no compromise has been reached. The ePrivacy Directive 2002/58/EC, most recently amended by Directive 2009/136/EC, therefore still applies.

The GPDR has already been followed by other regulations and directives that must be complied with for digital offerings and the handling of (personal and also non-personal) data, in particular the Platform-to-Business Regulation (EU) No. 1150/2019, the Free Flow of Data Regulation (EU) No. 1807/2018 and finally the Digital Content Directive (EU) No. 770/2019 and the Directive on Certain Contractual Aspects of the Sale of Goods (EU) No. 771/2019, dealing with goods with digital elements.

Implementation of the digital strategy picks up speed

For some months now, however, the new draft legal acts submitted by the Commission, some of which have already successfully passed through the legislative process, have been coming thick and fast. Some of these govern niche areas, others special topics, and still others are highly relevant to a wide range of players in the single market when dealing with digital products and services.

The most important regulatory areas of the current legislative processes concern the regulation of digital gatekeepers and the use of data („data strategy“). The Data Governance Act and the Data Act form the data strategy, while Digital Services Act and Digital Markets Act regulate the digital gatekeepers. Further relevant actions worth mentioning are the regulation of future topics such as Artificial Intelligence and finally, as a kind of backbone, Data Security.

Digital Gatekeepers: Two key actions of the digital strategy, the Digital Services Act and the Digital Markets Act, affect to online platforms in particular. The legislative process of both regulations is well advanced. The EP adopted both regulations on 5 July 2022 (P9_TA(2022)0270; P9_TA(2022)0269). The Digital Services Act includes new and revised rules that define the responsibilities and obligations of intermediary services, like online platforms. The Council did not approve the Digital Services Act yet. The Digital Markets Act complements competition law and limits the power of large platforms with significant network effects acting as gatekeepers. The Council approved the Digital Markets Act on 18 July 2022 (ST 11507 2022 INIT).

Data Strategy: The European Data Strategy (COM(2020) 66 final) is another key action of the digital strategy. The data strategy aims to make Europe a global leader in the digital economy and create a single European data space where personal as well as non-personal data, including sensitive data, can flow freely and securely across sectors (COM(2020) 66 final, p. 4 et seq.). One element, Regulation No. 868/2022, the Data Governance Act, came into force on 23 June 2022 (OJ L 152, 3.6.2022, p. 1-44). The new regulation aims to create a “legislative framework for the governance of common European data spaces” and to boost data business by lay down rules for re-use of certain categories of data held by public sector bodies (as a complement to the Directive No. 1024/2019, the Open Data Directive), data sharing and data altruism (COM(2020) 66 final, p. 12; COM(2020) 767 final; Recital 2 Data Governance Act). It is applicable in all Member States from 24 September 2023. In February 2022, the European Commission has proposed a Regulation on harmonised rules on fair access to and use of data, the Data Act, as another part of its data strategy (COM(2022) 68 final). The legislative procedure is ongoing. Currently, the member states are consulted during the first reading (https://kurzelinks.de/s89d).

Artificial Intelligence: People need to trust the technology itself, in particular Artificial Intelligence (AI). The aim is to create a legislative framework for trustworthy AI that strengthens trust in AI-based solutions and encourages development and investment in this field (COM(2020) 67 final, p. 5). In April 2021, the European Commission presented its AI package, including a Proposal for a Regulation laying down harmonised rules on Artificial Intelligence (AI Act: COM(2021) 206 final). The EU intends to take a pioneering role with the regulation of artificial intelligence. Despite many possible criticisms of the draft, the EU has succeeded in doing so if it manages to get the regulation off the ground in a timely manner. The legislative process is still in its first reading. Currently, the member states are presenting their opinions on the draft in the Council (ST 8364 2022 INIT).

Data Security: For all digital solutions, data security is a key factor for usability and trustworthiness. The experiences of the last months and years with many cyberattacks have sharpened the importance of this topic in the general public. To increase the trust of people and businesses that their applications and products are safe the digital strategy includes actions to build resilience to cyber threats (COM(2020) 67 final, p. 5). Therefore, on 16 December 2020 the European Commission adopted a Joint Communication to the European Parliament and the Council, the EU Cybersecurity Strategy for the Digital Decade (JOIN(2020) 18 final) which shows the way of the EU`s cybersecurity policies. On the same day, the European Commission also adopted a proposal for a revised Directive on Security of Network and Information Systems (NIS 2 Directive; COM(2020) 823 final). When the ongoing legislative procedure is completed, the new Directive will repeal the Directive No. 2016/1148 (NIS Directive) to deal with new challenges and threats generated by the digital transformation moving forward, which require adapted and innovative responses.

The interaction of the various legal acts

The various legal acts all concern digital offerings and products, the handling of data. They pursue different goals, but overlap. A major and justified criticism of the new legal acts is that they have not been coordinated in detail: most of them stipulate that other legal acts remain unaffected, especially the GDPR. Users must therefore examine all legal acts and implement their obligations. If there are ambiguities here because different legal acts do not result in exactly the same obligations, users must resolve such themselves, although this is originally the task of the legislator. The speed, the actionism and possibly also the challenge of finding political agreements have probably pushed this into the background.

This can be clearly seen, for example, in the definition of „data": While under GDPR, data is defined as „information" relating to a natural person (digital, analogue in whatever kind; Art. 4 (1) no. 1 GDPR), the new digital acts define data as digital representation of acts, facts, or information including compilations in forms as sound, visual or audiovisual recording (Art. 2 (1) Data Governance Act, Art. 2 (24) Digital Markets Act). For the definition of personal data, however, those acts refer to Art. 4 no. 1 GDPR. This leads to an unclear understanding of what „data" is, especially as the GDPR is supposed to take precedence in the event of a conflict. The differences in the definition of processing are less serious, but the GDPR is also open to analogue forms; the definition in the Proposal for the Data Act, for example, only refers to data „in electronic format" (Art. 4 (2)).

In particular, however, the insufficient connection between the new digital legal acts, especially also with the GDPR, leads to avoidable legal uncertainty. The new digital regulation is of considerable scope. It is already questionable whether more regulation can really lead to more innovation and a vibrant single market for data. This is even more questionable with the current design, which not only brings the enormous challenge of examining and implementing countless pages of legal texts for the actors. In addition, even with legal analysis by experts, uncertainties remain as to where, for example, which supplementary obligations apply and how individual requirements interact. This will have a paralysing rather than an invigorating effect.

What remains to be said is this: The digital strategy is pursuing an important and very correct goal. However, in the implementation, the actionism has apparently become so great that the multitude of legal acts with unclear relationships could lead to the goal achieved being reversed and instead of a more flourishing data economy, the new digital regulation could rather have the opposite effect.

Dr. Kristina Schreiber

ZEI Senior Fellow and Partner of Loschelder Law Firm, Cologne.

New Rules of Conduct under the DMA – Who are the “Gatekeepers” to Digital Markets?

Huge online platforms like Google, Amazon, Facebook, Apple, and Microsoft (“GAFAM”) have a significant impact on the internal market, providing gateways for a large number of business users to reach end users. In order to ensure contestable and fair markets in the digital sector, the Commission’s proposal for the Digital Markets Act (“DMA”) establishes new rules of conduct for so-called “gatekeepers” (European Commission 2020).

This article will examine the notion of gatekeeper (I.) with a focus on the interpretation of undefined legal terms (II.) and also in relation to similar terms that are applied in EU and German Competition Law (III.).

I. Notion of gatekeeper according to Art. 3 DMA

Whereas Art. 3 para. 2 DMA sets fixed thresholds for the designation of a gatekeeper, para. 1 allows for an individual assessment.

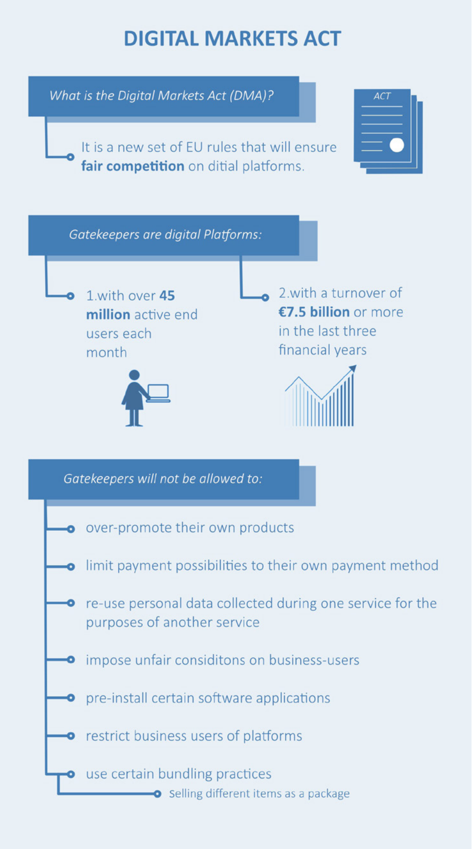
1. Art. 3 para. 2 and para. 5 DMA: Presumption of gatekeeper-status when certain thresholds are reached

The Commission will “without undue delay” (Art. 3 para. 4 sent. 1 DMA) designate an undertaking as a gatekeeper if that undertaking meets the thresholds laid down in Art. 3 para. 2 DMA. According to Art. 3 para. 2 DMA, the gatekeeper status is presumed, hence, the burden of proof is reversed (Recital No. 23 DMA). The gatekeeper-status is presumed if

(a) an undertaking achieves an annual EEA turnover equal to or above EUR 6.5 billion in the last three financial years, […] and it provides a core platform service in at least three Member States;

(b) it provides a core platform service that has more than 45 million monthly active end users established or located in the Union and more than 10 000 yearly active business users established in the Union in the last financial year;

(c) the thresholds in point (b) were met in each of the last three financial years.



DIGITAL MARKETS ACT

What is the Digital Markets Act (DMA)?

It is a new set of EU rules that will ensure **fair competition** on ditial platforms.

Gatekeepers are digital Platforms:

1.with over **45 million** active end users each month

2.with a turnover of **€7.5 billion** or more in the last three financial years

Gatekeepers will not be allowed to:

- over-promote their own products
- limit payment possibilities to their own payment method
- re-use personal data collected during one service for the purposes of another service
- impose unfair considitons on business-users
- pre-install certain software applications
- restrict business users of platforms
- use certain bundling practices
  - Selling different items as a package

(European Union 2022)

These thresholds will certainly be met by the “GAFAM” companies.

2. Art. 3 para. 1 DMA: case-by-case assessment

Regardless of these thresholds, companies can be classified as gatekeepers when they meet the qualitative criteria of Art. 3 para. 1 DMA. A provider of core platform services shall be designated as a gatekeeper if

(a) it has a significant impact on the internal market;

(b) it operates a core platform service which serves as an important gateway for business users to reach end users; and

(c) it enjoys an entrenched and durable position in its operations or it is foreseeable that it will enjoy such a position in the near future.

II. Interpretation of Art. 3 para. 1 DMA

Under Art. 3 para. 1 DMA, the gatekeeper status of an undertaking will be determined based on a case-by-case assessment in relation to other market participants. The criteria are openly formulated and contain undefined legal terms. In the following, these terms shall be interpreted particularly with regard to the recitals of the DMA.

1. Significant impact on the internal market

Art. 3 para. 1 lit. a DMA indicates that the undertaking must have a significant impact on the internal market. This depends on the market position of the company. According to Recital No. 25, several factors that determine the company’s ability to exert its influence on the internal market are to be taken into account, such as economies of scale, network effects, lock-in effects, multi-homing and vertical integration.

2. Core platform service which serves as an important gateway for business users

Art. 2 para. 2 DMA contains a list of “*core platform services*”. With regard to “GAFAM”, these are in particular online intermediation services, online search engines and online social networking services. However, with “*operating systems*” being likewise covered, many more businesses are potential addressees of the DMA.

The core platform service must serve as an important gateway for business users to reach end users. In line with Recital No. 20, business users depend on a central platform service provided by a gatekeeper in order to reach a large number of end users. It is therefore necessary to compare the number of end users that the business users reach with and without the support of the core platform of a gatekeeper.

3. Entrenched and durable position

According to Recital No. 21, the feature “*entrenched and durable position*” refers to the contestability of the position. It is irrelevant how long the company has held a dominant position. Rather, it is decisive whether the position the company currently holds can be contested by competitors. As the position can be influenced by market developments and technical developments, the Commission should be empowered to adopt delegated acts, laying down methods to determine whether certain quantitative thresholds are met. As per Recital No. 25, particularly important parameters when assessing the (future) contestability of the company’s position are market capitalisation and growth rates.

III. Comparison

The DMA pursues an objective that is complementary to the aim of protecting undistorted competition on the market, as defined in competition law terms (Recital No. 10). Therefore, the DMA’s notion of gatekeeper should be compared to how digital platforms are dealt with under Sec. 19a GWB and Art. 102 TFEU.

1. Gatekeepers under Sec. 19a GWB

With the latest amendment in 2021, the German legislator introduced Sec. 19a of the German Competition Act (“GWB”) in order to “*prohibit big tech companies from engaging in certain types of conduct much earlier*”. By this, the German legislator has preceded the EU legislator and assumed an “*international pioneer role*” (Federal Cartel Office 2021).

According to Sec. 19a para. 1 GWB, the Federal Cartel Office determines whether a company is of “*paramount significance for competition across markets*”. Sec. 19a para. 1 sent. 2 GWB lists criteria, including the dominant position on the market (No. 1), to be included into the assessment of the authority. If the Federal Cartel Office has determined that a company is of such significance, within its discretion, it can prohibit certain types of behaviour in accordance with Sec. 19a para. 2 GWB, thus enabling an early intervention.

In line with the “*pioneer role*” of the German legislator, the Regulation largely corresponds to Art. 3 DMA. However, Sec. 19a GWB is more general and does not specify any thresholds.

2. Gatekeepers under Art. 102 TFEU

Art. 102 TFEU applies to undertakings of a dominant position within the internal market or in a substantial part of it. According to the European Court of Justice, a company has a dominant position if its “*position of economic strength […] enables it to prevent effective competition being maintained on the relevant market by giving it the power to behave to an appreciable extent independently of its competitors, customers and ultimately of its consumers*” (European Commission, Case C-27/76, para. 66).

The decisive criterion for determining dominance is the company’s market share. In this context, the fact that digital markets are partly free of charge constitutes a major challenge (Crémer et al. 2019) and bears the risk of a loophole in competition law.

3. Conclusion

In sum, the DMA’s notion of gatekeeper is narrower than the terms “*paramount significance for competition across markets*” (Sec. 19a GWB) and “*market dominance*” (Art. 102 TFEU). With regard to the regulatory scope, the DMA and Sec. 19a GWB are sector-specific, while Art. 102 TFEU applies to the entire internal market. Finally, the regulatory purposes are different: While Sec. 19a GWB and Art. 5 to 7 DMA, having a preventive effect, impose *ex ante* obligations on gatekeepers, Art. 102 TFEU enables ex post intervention once a dominant position has been established.

IV. Outlook

Regulatory and competition law are designed to complement each other. In view of the differences in their scope of *application ratione temporis (ex ante v. ex post)*, Art. 1 para. 6 and 7 DMA contain conflict of law provisions that distinguish between regulatory and competition law. Given their complementary objectives, the DMA, Sec. 19a GWB and Art. 102 TFEU should be applicable side by side.

The DMA and Sec. 19a GWB intend to limit the power of the most important and largest influencing companies, especially the “GAFAM” companies, in order to prevent damage caused by market abuse beforehand. Eventually, authorities may not have to intervene as often and resources can be used elsewhere. However, the effectiveness of the new regulatory instruments is yet to be proven in practice.

Hannah Döding

Student Assistant, Faculty of Law and Political Science, University of Bonn.

Krisztina Mezey

ZEI Research Fellow and PhD candidate in Law at the University of Bonn under the supervision of Prof. Christian Koenig.

DSA - Strong internet legislation bonds societies

The Russian war of aggression shows how dangerous targeted disinformation campaigns can be. When hate and disinformation set the tone online, dictators, autocrats and tycoons can abuse it to undermine democratic values and even justify a war to their own people. This cannot be tolerated. The Digital Services Act (DSA) will mark a turning point in this regard, stipulating globally applicable rules and obligations for digital platforms for the first time with a view to defending our fundamental rights and democracy.

Shoshana Zuboff, the inspiring Harvard economist, described the impact of the DSA with a strong image: “The European member states, their parliament, the EU Commission and the European council together set ablaze the beacons that rim the mountain peaks and proclaimed to the world that democracy is back.” This hope can give rise to a Digital Spring, setting increasingly stringent laws the world over.

What specific achievements have we already made in Europe?

National court orders and decrees have to be consistently implemented, dispelling the impression that the internet is a lawless space. Moreover, the days of each platform having free rein over their T&Cs and content moderation are now gone, with all platforms obliged to implement non-ar terms and conditions. Should Elon Musk be minded to reactivate Trump’s account, it will have to be done in line with the same rules for all other users.

The pioneering nature of the DSA is in its provisions for the very large platforms with over 45 million users, though. It does not hold the platforms liable for their users’ opinions, but rather for their own actions. The DSA obliges large platforms such as Google, Meta or Twitter to assess their algorithms for risks to fundamental rights, i.e. non-discrimination and the preservation of freedom of expression – entirely irrespective of who they are owned by. So, Elon Musk will also have to abide by these rules if he wants Twitter to remain successful in Europe. The attention-based ranking system which fills the pockets of corporations through disinformation, hate and agitation will thus be put to the test. Until now, the loudest and most outrageous posts that generate the most interactions are given more visibility because they keep people in front of their screens. Platforms like YouTube and Facebook have so far reaped the rewards by generating more advertising revenue through longer viewing times, and we have put up with powerful corporations maximising profits to the detriment of our societal values. The DSA will shed a light on those practices and open up avenues for remedies.

The DSA will be the new constitution for the internet and for the first time independent scientists and – to a lesser extent – NGOs will be granted insight into the platforms’ mechanisms to assess the risks for society from the outside. The DSA will ensure more cohesion in society with this safety net. Anyone who nevertheless upholds their divisive mechanisms with rabble-rousing news, fake videos and hate speech to increase the time users spend on their sites and maximise their own advertising revenues will have to reckon with tough opposition.

For the first time, clear legal limits shall be set on the tapping of our personal data for advertising purposes. Sensitive personal data such as religion, skin colour or sexual orientation may no longer be used for profiling for advertising purposes. Likewise, children’s and young people’s data may no longer be accessed for this purpose. This is a huge success because with it we are also promoting the development of alternative forms of advertising.

I am fighting for a complete ban on behaviour-based tracking because also it simultaneously enables hate, agitation and disinformation to be spread online. The data serves as a breeding ground for disseminating manipulative messages and content to vulnerable target groups according to the same principles as advertising. Once they have gained sufficient acceptance in online groups, those groups organically spread them online until they find their way into more and more minds and public discourse. Such advertising mechanisms thereby exacerbate the polarisation of our society and undermine our democracy. Powerful and financially influential individuals can deliberately exploit these situations. That is precisely how Putin’s henchmen are also able to manipulate certain population groups in Western countries. The DSA is a first defence against this practice.

The essence of the DSA, namely putting an end to surveillance advertising and online platforms’ manipulative practices that peddle hate, agitation and disinformation, strengthening users’ rights and holding online platforms to account like never before, will make it a unique constitution for the digital world. It will change our lives, society, and the internet. It will bestow us more democracy and freedom, giving democratic societies the power to thrive in the digital age.

Alexandra Geese, *Member of the European Parliament.*

Interview with Alexandra Geese

Alexandra Geese

Alexandra Geese, German Member of the European Parliament, was the Green Group rapporteur for the Digital Service Act. Geese, who is an interpreter by profession, has been a member of the Greens/EFA group since the 2019 European elections. She is a member of the Committee on Budgets and the Committee on the Internal Market and Consumer Protection. (Photo: Sandra Then)

Mrs Geese, in your article, you write that companies that make money from hate, agitation and social division must expect tough resistance. What exactly does this resistance look like against companies that do not comply with the new regulations? What types of sanctions do you think will be particularly effective and lead to a significant change in corporate behaviour?

The revolutionary thing about the Digital Services Act (DSA) is that, unlike the NetzDG, it does not focus on individual content, but really on the actions of the platform itself. Through the risk assessment that the platforms have to carry out, which is then independently verified, and through the fact that the Commission, the supervisory authorities and independent researchers are finally being given access to the platforms' data, we can now look at how exactly hate and incitement are spread for the first time. Until now, we had the impression that the internet is much worse than the analogue world in terms of hate speech. But it always remained just a feeling based on anecdotal evidence and small studies. Without any real insight, a Mr Zuckerberg can always stand up and say "that's not true at all". Now that we have this access to data with which we can check how the algorithms work, we can really understand which content is particularly amplified and particularly promoted and, above all, why. The moment we know exactly which mechanisms are at work, we can readjust accordingly. The readjustment can then be done in different ways. The easiest way is, first of all, through the "Codes of Conduct". These are self-regulatory instruments coordinated by the Commission. They exist on disinformation and on countering illegal hate speech online. Very specific obligations can be written into them, for example, how certain algorithms may or may not function. Accordingly, there may be explicit rules on the way algorithms prioritize content. The platforms then sign this mechanism and adhere to it in a legally binding way. In the event that the platforms violate the "Codes of Conduct", the DSA provides for sanctions.

Sanctions in the form of fines and penalties?

Exactly, in the form of fines that last as long as the platform‘s illicit behaviour continues. That means there can be quite a bit of money involved. However, all of this does not deprive us of the possibility that if it is evident that the illicit behaviour is leading to particularly strong breaches, we can first collect evidence and then, again, initiate very targeted legislation. But, under the DSA, you can initially punish with targeted fines. What is also important, especially in view of the German debate, is that with the DSA there must be a mandatory legal representative in Europe. Accordingly, the Telegram case cannot be repeated.

Given that the Digital Services Act does not explicitly define what illegal content is, could you give us some examples of online content that should be removed? You have already mentioned that it is particularly about understanding and managing the big picture, but is there nevertheless specific content that needs to be removed in any case?

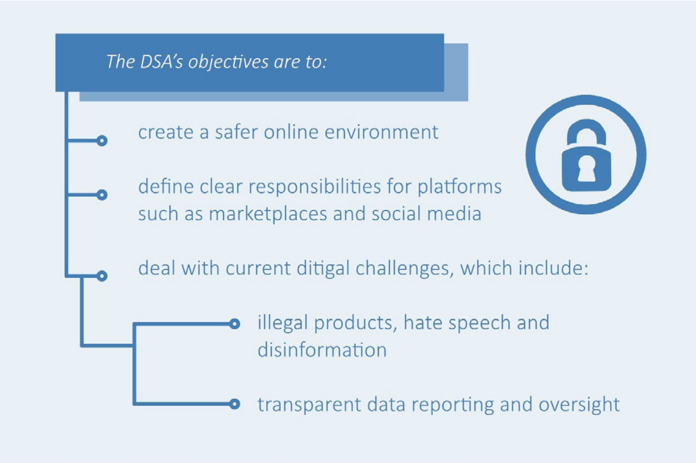
Yes, you have to separate these two issues. There are rules in the first case about individual illegal content and how to deal with it. What constitutes illegal content is not defined by the DSA – we have no legislative competence for that on the EU level – but is defined by the individual member states. To give a simple example, in Germany, for example, Holocaust denial is illegal, i.e. posts that contain Holocaust denial are forbidden and must be removed immediately upon a simple request. The platform in question must react immediately; they cannot drag this out. The same content is not illegal in Denmark, however, where it remains on the net. The same material is not legal or illegal in all countries. But that in turn gives the member states the possibility to decide what is illegal and what is not. Entirely in accordance with the principle of subsidiarity, not because it were defined by the DSA. It is about enforcing existing rules on illegal content. That‘s where the big problem has been so far; the difficulty of enforcing them, because platforms have used any kind of pretext for their inaction, or, on the contrary, have removed legal content. Now there are clear rules for this.

A particularly well-known buzzword in connection with digital legislation is upload filters. In the DSA, there is an explicit "prohibition of monitoring obligations by platform operators". Does that mean that upload filters are no longer an issue under the Digital Service Act?

No, that is quite clear. Of course, the copyright directive remains, but we are not introducing any upload filters with the DSA. There was also a very clear consensus on this.

Then I would like to focus on the future. Do you think that other countries, such as the US, will follow the EU's example and enact new regulation that will limit the supremacy of gatekeepers, ensure law enforcement on the internet and protect democracy?

In the US, this debate is very complex. I know that many people involved in this issue are looking at Europe with great interest. Among them, for example, the President of the FCC (Federal Communications Commission) Jessica Rosenworcel in the US. Whether there will be legislation or not, I can‘t say. I know that there are many different proposals in Congress, but whether any of them will find a majority is difficult to assess. I have the impression that, at the moment, the debate in the US is very much focused on the monopoly situation. It has become obvious that there is actually no competition in the sector any more. Instead, some have a clear monopoly position, against which young, fresh competitors hardly stand a chance. A new business model is immediately bought up in some form or the other. Therefore, my feeling is that in the US, the approach is more to regulate these monopoly issues and to restore competition. In addition, there are also some proceedings going on in the US regarding the advertising industry. These make it clear that Google and Meta control the advertising market: They control 80 per cent of the advertising market in Germany and even more in the US. As part of 12 different lawsuits, a whole lot of official documents were disclosed, which show that Google and Meta have worked very closely together in this area and basically form a cartel and prevent new, more innovative forms of advertising delivery. There is also always the big debate about the liability of the platforms, the question of responsibility. However, I think this is too short-sighted, which is why we have solved the problem in Europe in such a way that we have not changed the liability provisions, but we are looking at the systemic issues. The platforms are still not liable for the content produced by their users as far as they have no knowledge of it. The central issue is what the platforms actually do with the content of the users. At the moment, the EU's legislation is the only one in the world that is really looking at this, and I find that remarkable. But there is also a lot of interest from other countries besides the US, which is why I believe that we have really created a model legislation for the democratic world.



The DSA's objectives are to:

- create a safer online environment
- define clear responsibilities for platforms such as marketplaces and social media
- deal with current ditigal challenges, which include:
  - illegal products, hate speech and disinformation
  - transparent data reporting and oversight

(European Union 2021)

Have countries outside the Western world also expressed interest?

I have also received enquiries from Japan, for example. There is interest from India, Pakistan, Australia and many other countries. In the digital field, there is another camp, China, which has completely sealed itself off and shortly prior to the EU, also presented its own legislation. But a totalitarian state cannot be a model for us, especially when it comes to data. Instruments with which a population can be controlled are exactly what we don‘t want. Therefore, in the area of digital legislation, there is really only the EU. The world is already watching. It is now a question of enforcement, whether we really enforce our rules consistently and really work well with them.

According to you, the DSA is "a first defensive measure". What will or must be further defensive measures to be implemented in the coming years?

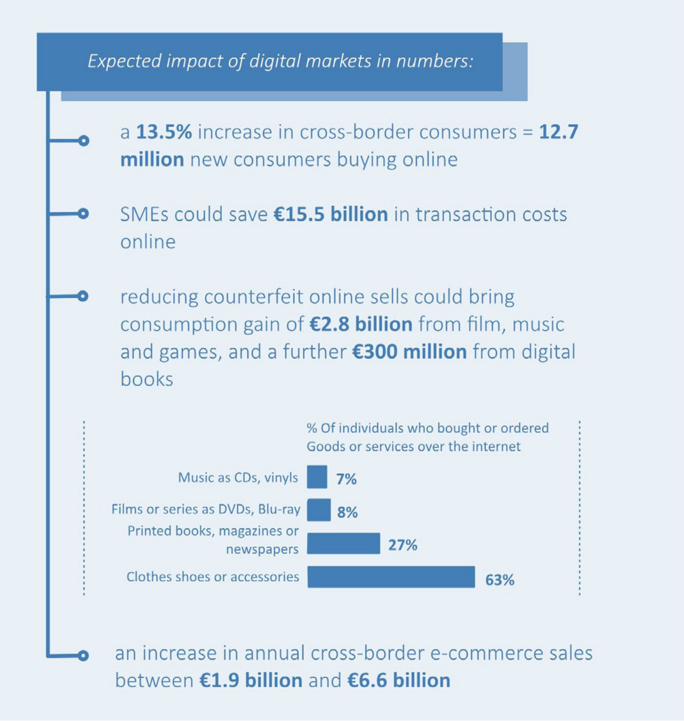
I see two measures and for the first one in particular I have also fought a lot. What we have seen in the course of working on this law is that the root of phenomena like disinformation or hate speech, that we are trying to combat, is the fact that our data is being snatched from us. We have to, when we surf the internet, regularly click on, for example, these cookie banners, because you don‘t really have an alternative, because there is never a „no“ button. As a result, an enormous amount of our personal data ends up with Meta and Google, but especially with many data brokers. The data is compiled into huge profiles about billions of people, which are really very comprehensive. This is done in the interest of advertising, but also to distribute very targeted content. Therefore, these data profiles naturally have incredible potential for abuse. If we think of Russian disinformation, for example, they reach people who are particularly susceptible to certain topics. We have now enshrined in the DSA that sensitive data according to the GDPR and data of children and young people may no longer be used for these advertising profiles. That is already a good first step, but it does not go far enough. The use of data profiles must be completely banned, not only for advertising purposes, but also for the recommendation mechanisms of the platforms. And with that, we come to the second point, the content that is selected by the platforms. We are no longer in the internet of the 90s, where you look for the content yourself, but the various platforms such as Twitter, Facebook, Instagram and TikTok provide us with a ‚feed’. In other words, you no longer see what you have selected yourself, but what the platform selects for you and the platform selects content that keeps you on the platform for as long as possible. The basis for this is provided by the aforementioned data profiles, which is why everyones timeline is different. It is known that people stay longer online somewhere, if they become active, i.e. if they interact on the platform. Psychological research shows that people are more likely to interact with content on the internet when negative emotions, such as fear and anger, are triggered. Subsequently, a self-optimisation of the algorithms takes place, because they register that content that upsets people in a negative sense works particularly well and people interact with it and stay longer on the platform. If people stay longer, more advertising can be displayed, and the platform earns more money. That‘s why the algorithms are optimised or optimise themselves in such a way that everyone gets to see what fits their worldview on the one hand and upsets them on the other. Which is an extremely problematic mechanism that needs to be levered out. But in order to do that, we first really need to understand how exactly this works, which is why we need data access and more research in this area. What the DSA now enables.

Given the rapid technological development, is there a way to ensure that regulation is future-proof and does not have to be reformed again in a few years because it lags behind the technological reality?

Yes, through data access in combination with the application of the statutory articles of the DSA, in the area of platform risk assessments. This combination makes the DSA a very dynamic legal instrument. Not only is illegal content identified and deleted, but instead, a dynamic assessment takes place every year to identify what the current dangers, risks to democracy, fundamental rights or children are. On this basis, measures have to be proposed and implemented. This makes it very dynamic, as measures can be taken directly on the basis of Article 27 of the DSA or, as mentioned, the „Codes of Conduct“ can be adapted. Or, in case of doubt, the law can be adapted at some point, but I don‘t see the necessity for the time being.

When it comes to legislation in the digital sphere, one quickly gets the impression that politics has a hard time adapting new things and regulating them quickly. The internet has been used commercially for more than 20 years now and it still takes time for real law enforcement to be created in the digital space. Why is that?

There are several reasons for that. Part of it is that you have a surface, but it doesn‘t really correspond with what‘s going on behind it. Very few people know what‘s going on behind the scenes, and the platforms are naturally very careful to be non-transparent and to keep the mechanisms secret. It is not easy to get to grips with the technical content. I dug into it relatively deeply and was also very surprised. I learned a lot there and what I learned is not always easy to explain. This makes it a very thankless political issue. You can‘t secure popularity or re-election with it. The same goes for data protection, you don‘t make yourself popular with that either. Which is why it is of course not an incentive for politicians to deal with this matter very intensively. On the other hand, there is a small but very clear lobby that prevents progress in this area, especially on data protection. Unfortunately, this includes not only Meta and Google, but also the publishers here in Germany and all over the world, who are entangled in this system and therefore defend it. This makes it very difficult to organise political majorities for digital legislation.



Expected impact of digital markets in numbers:

- a **13.5%** increase in cross-border consumers = **12.7 million** new consumers buying online
- SMEs could save **€15.5 billion** in transaction costs online
- reducing counterfeit online sells could bring consumption gain of **€2.8 billion** from film, music and games, and a further **€300 million** from digital books

- an increase in annual cross-border e-commerce sales between **€1.9 billion** and **€6.6 billion**

(European Union 2021)

One last remark: There is a clear connection, even if we cannot prove it yet, but it is obvious, between the way social networks work, the business model based on hate and agitation, and the rise of far-right governments. Otherwise, there is no other way to explain what is happening in Sweden, Italy, the Philippines and elsewhere in the world. There are, for example, very interesting contributions by Maria Ressa, winner of the Nobel Peace Prize 2021. Unfortunately, you have to see the connection. This also makes it much more exciting for the future of Europe. I see this as a very big threat, which is why the Digital Services Act is so important.

(Translated from German into English by Henrik Suder)

The Broadband Guidelines 2022 - New opportunities for accelerating the roll-out of gigabit-networks through State subsidies?

In December 2021, the European Commission published the draft Broadband Guidelines 2022, a key instrument for the future of state-subsidised broadband deployment. Through the Guidelines, Member States may, under certain conditions, support infrastructures where there is no incentive for private investment.

The Guidelines do not constitute a legal act within the meaning of Article 288 TFEU. Nonetheless, there is a self-binding effect due to the principle of equal treatment and the protection of legitimate expectations under public law. In this context, the Guidelines specify the European Commission's Balancing Test (Article 107(3) c) TFEU).

All in all, the Broadband Guidelines set out the legal framework for state aid in the broadband sector. Initially, the adoption of the new Broadband Guidelines 2022 was foreseen for mid-2022. At this point in time, however, the new Guidelines still remain in the drafting process.

I. Revision of the Broadband Guidelines 2013

Currently, the Broadband Guidelines 2013 (2013/C 25/01) still define the legal framework for State aid in the broadband sector. According to the Guidelines, public investments are allowed if there is a market failure, and the investments bring about a step change.

Due to the technological progress and the increased digital networking needs, the European Commission launched a public consultation in 2020 in course of a proposed revision of the EU State aid rules for deployment of broadband networks. The Broadband Guidelines 2013 are based on the former connectivity goals as set out in the *Digital Agenda for Europe* (COM (2010) 245 final) in 2010. Accordingly, the legal parameters are no longer compatible with the current objectives, which focus on gigabit connectivity (see ZEI Future of Europe Observer Vol. 10 No. 1/2022, p. 5). Against this background, a revision, and adaption of the Broadband Guidelines is necessary to further accelerate the roll-out of FTTH-networks and 5G.

As a result, the draft Broadband Guidelines 2022 show harmonisation with the current policy and priorities of the European Commission (*Green New Deal, European Gigabit Society 2025, Digital Compass 2030*) as well as with market and technology developments.

II. New Legal Framework under the Broadband Guidelines 2022

Basically, the Broadband Guidelines 2022 introduce new take-up thresholds for public funding of gigabit fixed networks. The aim of the new take-up thresholds is to reflect the increasing connectivity needs of end-users and to clarify the requirements for granting aid (see 1.).

Furthermore, demand-side measures to promote the use of fixed and mobile networks (vouchers) have been added. Until now, the Commission did not consider demand-side subsidies as measures falling within the scope of the Broadband Guidelines (see Commission Decision of 7 January 2019 - SA. 49935 (2018/N) – *Greece Superfast Broadband (SFBB) Project*). The purpose of the extension of the scope of application is now, to ensure legal certainty by clarifying the parameters that the Commission applies in relation to these measures based on recent case practice (see 2.).

1. Supply-side Subsidies

Regarding supply-side subsidies, the Broadband Guidelines 2022 set out two main requirements. First, the aid measure has to be necessary, i.e. there must be a market failure. In addition, the aid measure must be an appropriate policy instrument. This is the case if a step change occurs.

a. Market Failure

To determine whether there is a market failure, the current connectivity situation in the target area must be considered. In this context, the new take-up thresholds must be taken into account. In order to implement the objectives of the *Gigabit Communication* (COM(2016) 587 final) and the *Digital Compass Communication* (COM(2021) 118 final), the thresholds have been adjusted. Accordingly, there is a market failure if the market does not and is not likely to provide users a connection with at least 1 Gbps download and 200 Mbps upload speed.

In this context, the Broadband Guidelines 2022 still differentiate between various areas in order to specify the requirements for the necessity of state aid. Thus, the basic concept of the Broadband Guidelines 2013, consisting of a classification of the target area to determine the necessity of an aid measure, is maintained. In any case, a market failure exists if there is no ultrafast broadband network providing at least 100 Mbps download speed ("white area"). If there are one ("grey area") or more ("black area") ultrafast broadband networks, market failure can only be proven, if these networks do not provide gigabit connectivity (at least 1 Gbps download and 200 Mbps upload speed). Therefore, compared to the Broadband Guidelines 2013, particularly subsidies in black areas continue to be an exception but are tied to significantly reduced requirements.

In order to classify the target area and identify a market failure, Member States must determine, on the basis of mapping and public consultation, whether ultrafast broadband networks already exist or are likely to be developed within the relevant time horizon in the target area. This ensures priority for privately funded deployment; State aid is therefore only eligible if the market cannot bring forward the envisaged connectivity on its own.

b. Step Change

Under the Broadband Guidelines 2022 a step change means a significant improvement delivered by the State funded networks, bringing substantial new infrastructure investments in the electronic communications networks and significant new capabilities to the market in terms of broadband service availability, capacity, speed, or other relevant characteristics of the network and competition. In order to determine whether a step change exists, the classification of the target area based on the current development situation is taken into account. Here, the download speed plays the most important role.

In white areas, where the existing infrastructure provides less than 30 Mbps download speed, the public support must at least double the download speed and at least reach 30 Mbps download speed. If the existing network provides at least 30 Mbps download speed, the public support must at least triple the download speed and at least reach ultrafast download speed. In grey areas, public support for a more performing network may only be granted if the State funded investment in the new network at least triples the download speed and sufficiently increases the upload speed as compared to the existing infrastructure. In black areas a step change exists if, in addition to the requirement of at least tripling the download speed and sufficiently increase the upload speed as compared to the existing network, the new network provides at least 1 Gbps download speed.

2. Demand-side Subsidies

Voucher schemes aim to increase the take-up or to incentivise end-users to maintain the subscription to fixed or mobile services. The measures are designed to reduce the costs for end-users. Due to the limit value of most vouchers, the aid is regularly *de minimis*. Where *de minimis* thresholds are exceeded, the Broadband Guidelines contain additional requirements for the State aid-compliant design of voucher schemes.

A distinction is made between social vouchers and connectivity vouchers. Social vouchers aim to support certain individual consumers to procure or maintain fixed or mobile services. They can be found compatible with the internal market on the basis of Article 107(2) a) TFEU. Thus, the vouchers must have a social character and be reserved for particular categories of individual consumers, whose financial circumstances justify the payment of aid for social reasons (for example lower income families, students, pupils, etc.).

Connectivity vouchers address broader categories of end-users (for example vouchers for all citizens or certain undertakings, such as SMEs). In order to be compatible with the internal market on the basis of Article 107(3) c) TFEU, such measures must contribute to the development of an economic activity and must not adversely affect trading conditions to an extent contrary to the common interest. Connectivity vouchers may only be made available in areas where at least one existing network is capable of providing the eligible service. This must be verified through mapping and public consultation.

III. Conclusion and Outlook

Overall, the Draft Broadband Guidelines 2022 show a successful alignment of the state aid framework with the new connectivity goals of the EU. In particular, the expanded possibilities for subsidies in black areas, as well as the legal certainty provided with regard to demand-side subsidies, should significantly accelerate the expansion of broadband in the future.

As soon as the Commission has finally adopted the new Broadband Guidelines 2022, the Member States should therefore take advantage of the new innovation perspectives and establish new aid programmes.

Carlos Deniz Cesarano

ZEI Research Fellow and PhD candidate in Law at the University of Bonn under the supervision of Prof. Christian Koenig.

Filipa Sacher

ZEI Student Assistant and Law Student at the University of Bonn.

Should content and application providers contribute a fair share to telecom network costs?

In 2021 European telecom network operators (ETNO) demanded that large content and application providers (CAPs) make an appropriate financial contribution to the expansion and modernisation of broadband infrastructure (ETNO 2021). Since a fair compensation of the telecom network operators could not be ensured in the currently unregulated interconnection markets, they advocate for a regulation at EU level. Telecom network operators prefer a model that functions according to the "sending-party-pays"-principle and would thus implement a contracting obligation between large CAPs and telecom network operators. This paper discusses the arguments for and against such regulation (I.), in particular whether such regulation violates net neutrality (II.).

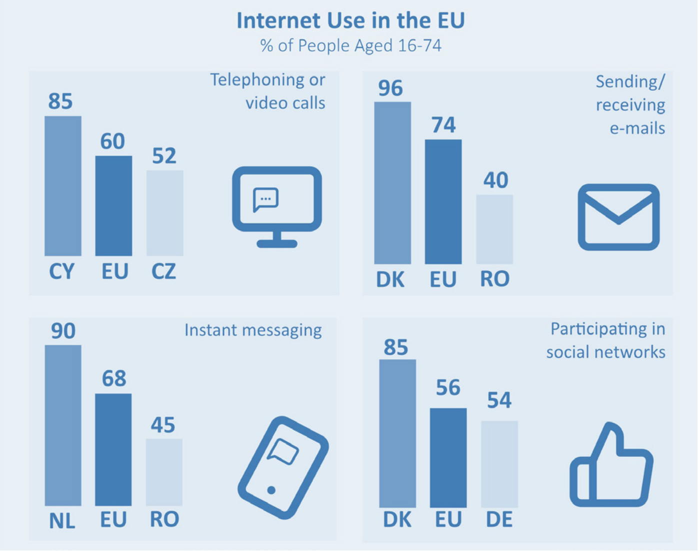
I. The conflict between telecom network operators and CAPs

Based on an account of the interest-driven conflict between telecom network operators and large CAPs, the arguments for and against such regulation are contrasted below.

1. The view of telecom network operators

Telecom network operators see the use of their infrastructure by large CAPs as a free ride, as telecom network operators would be unable to negotiate fair commercial terms for the use of their networks. More than 50 per cent of data traffic in Europe's telecom networks come from four global internet companies (FANG) (Hristov 2022), which have considerable bargaining power over telecom network operators because their content is indispensable to end users. Due to these market conditions, it would be hardly possible for network operators to receive adequate compensation for their steadily increasing investments in modern fibre infrastructure.

At the same time, regulation that obliges large CAPs to make an appropriate contribution for the use of telecom infrastructure could promote the achievement of political goals. In 2021, the EU Commission formulated the ambitious goal of ensuring gigabit connectivity throughout the EU by 2030 (COM (2021) 118 final) and in this context emphasised its efforts to ensure a fair distribution of costs: "*We commit to [...] developing adequate frameworks so that all market actors benefiting from the digital transformation [...] make a fair and proportionate contribution to the costs of public goods, services and infrastructures*" (COM (2022) 28 final, p. 3).



(Eurostat 2020)

Usage-based payments by large CAPs could not only serve to expand and modernise the infrastructure, but also contribute to the creation of an economic incentive to ensure data efficiency and thus prevent congestion in broadband networks within the EU. Currently, networks in the EU are generally capable of handling the volumes of data transmitted over them. During the COVID-19 pandemic, however, the EU Commission had to rely on the goodwill of major streaming providers to lower the quality (and thus the bandwidth usage) of their video streams to prevent network congestion due to the significant increase in demand for their content (Lomas 2020). Given the exponential growth in the amount of data transported over broadband networks, according to telecom network operators, there is a very real risk of widespread capacity bottlenecks in the near future (Gajek 2022).

Both the expansion of energy- and resource-efficient infrastructure and the implementation of an economic incentive for data efficiency could also significantly reduce electricity use and thus CO2 emissions. For example, a Germany-wide fibre-optic supply could save up to 1,100 megawatts of electrical power per gigabit of data compared to copper-based networks (Obermann 2022). Using the broadband infrastructure in a way that conserves resources as much as possible by reducing or keeping the data volumes transported over networks to a minimum also holds considerable potential for reducing energy consumption in the telecom sector (Kersting 2020).

2. The view of CAPs

Large CAPs naturally oppose the efforts of the telecom network operators. In particular, they are of the opinion that the interconnection markets are functioning and should therefore not be regulated. In addition, they claim that they already make sufficient payments to increase the overall capacity of telecom networks, for example through the expansion of content delivery networks, which host their content in a Member State and are either integrated into telecom networks (enter-deep-strategy) or interconnect directly with network operators via peering relationships (bring-home-strategy) (Neumann et al. 2022). In any case, there would be no free ride, since the demand for content also increases the revenues of network operators or ISPs in the area of internet access services, which thus creates a mutually beneficial interdependence. Also, the vast majority of network costs are concentrated in the access network ("last mile"), which costs grow proportionate to the number of subscribers, not to the amount of traffic (European VOD Coalition 2022). At the same time, the innovations in the area of data compression suggest that there is already a sufficient incentive for data efficiency. For example, Netflix uses "encoding" to show the same video with fewer and fewer bandwidth requirements and has been able to increase the number of hours a subscriber can stream per GB of data by 200 per cent over the past 5 years (Netflix 2021).

II. In particular: violation of net neutrality?

The obligation of CAPs to make direct payments to network operators for the termination of their data is also seen as a violation of net neutrality. In this context, Art. 3 Regulation (EU) 2015/2021 states:

> „*1. End-users shall have the right to access and distribute information and content, use and provide applications and services, and use terminal equipment of their choice, irrespective of the end-user's or provider's location or the location, origin or destination of the information, content, application or service, via their internet access service.*
>
> *[…]*
>
> *3. Providers of internet access services shall treat all traffic equally, when providing internet access services, without discrimination, restriction or interference, and irrespective of the sender and receiver, the content accessed or distributed, the applications or services used or provided, or the terminal equipment used. […]*"

It should be noted, however, that "net neutrality" is neither a fixed legal concept nor a legal principle under Union primary law, but is only in expressed in secondary law, and therefore – apart from an obligation to ensure the coherency of secondary legislation – does not set any direct requirements for the legislator when creating secondary law.

Net neutrality is at its core a technical concept based on the internet's best-effort-principle with regards to the transmission of data, but the exact legislative form it should take is extremely disputed in the literature and, from a global perspective, has been regulated by legislators in a wide variety of ways. An obligation for large CAPs to make direct payments to telecom network operators regulated by law, would thus merely represent an adjustment of the Union's understanding of net neutrality and, strictly speaking, could technically not violate "net neutrality" at all, provided the Union legislature decrees that the contracting obligation requirement takes precedence over the provisions of the Regulation (EU) 2015/2021. Whether such an understanding, on the other hand, corresponds to a morally desirable design of a "neutral and open internet" (COM (2022) 28 final, p. 3) is a different question, which is – provided there is no obvious violation of the principle of proportionality under Union law (Art. 5 para. 4 TEU) – not of legal, but political nature.

III. Outlook

In May, internal market commissioner Thierry Breton announced that the EU Commission would present a proposal before the end of the year that would force platforms to pay a "fair contribution" to developing digital infrastructure such as 5G networks (Bertuzzi 2022). In view of the arguments put forward so far, which can largely be traced back to network operators' or CAPs' own interests, as well as the potential economic impact of such regulation, it seems indispensable to carry out comprehensive market studies and consultations with all relevant stakeholders. Accordingly, in a letter dated 19 July, some Member States also warned against any hasty decisions on this matter: "*Policy changes affecting relationships between telecom operators and platform providers need to be carefully examined on all aspects and considered by engaging all the relevant stakeholders*" (Bertuzzi 2022).

Anton Veidt

ZEI Research Fellow and PhD candidate in Law at the University of Bonn under the supervision of Prof. Christian Koenig.

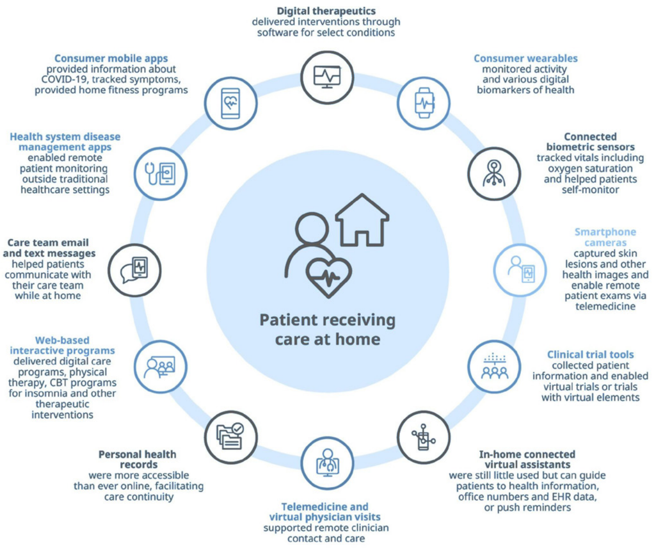
Digital Healthcare: Acceleration due to the pandemic

The relevance of health policy has increased immensely recently. For each individual, but also for the EU as a whole. In the light of the COVID-19 pandemic, the European Union is showing great interest in protecting its citizens from future pandemics. This is why the EU is looking for a unified healthcare system across Europe to deal with a pandemic like the one we have experienced in recent years, instead of each Member State dealing with it individually. Healthcare is constantly dealing with multifaceted complexities, politically, economically, and socially. This results in enormous implementation restrictions, coordination, and harmonisation difficulties for EU legislation, but also a multitude of competing solutions. Digitisation plays a decisive role in these.

The problems of the current health system

The current situation requires a change in thinking that sees health as an investment rather than a cost. With regard to the ageing population, EU institutions emphasise improved digital health surveillance that tracks and monitors the ageing population via links to nearby healthcare systems for emergencies (Expert Group on Health Systems Performance Assessment, 2020). Health surveillance in this form has so far been very poor. In this context, digitisation brings with it health promotion and a caring attitude, which plays a vital role in the Commission establishing new guidelines to enable authorities and hospitals to pool the work or beds of their healthcare staff. This would make health care more efficient and ensure better care that would counteract the shortage of skilled workers. Public hospitals need to take basic measures to ensure sufficient nursing staff and improved citizen communication. The destructive impact of the pandemic on health workers in terms of overwork came at a time when many EU countries were facing labour shortages, making them even more acute. A multifaceted approach to preventative medicine, bolstered by the safety net, is essential to achieving and maintaining public health's curative status (Greer et al., 2022).

Digital Health Tools in the Patient Journey During the COVID-19 Pandemic


Digital therapeutics delivered interventions through software for select conditions
Consumer wearables monitored activity and various digital biomarkers of health
Connected biometric sensors tracked vitals including oxygen saturation and helped patients self-monitor
Smartphone cameras captured skin lesions and other health images and enable remote patient exams via telemedicine
Clinical trial tools collected patient information and enabled virtual trials or trials with virtual elements
In-home connected virtual assistants were still little used but can guide patients to health information, office numbers and EHR data, or push reminders
Telemedicine and virtual physician visits supported remote clinician contact and care
Personal health records were more accessible than ever online, facilitating care continuity
Web-based interactive programs delivered digital care programs, physical therapy, CBT programs for insomnia and other therapeutic interventions
Care team email and text messages helped patients communicate with their care team while at home
Health system disease management apps enabled remote patient monitoring outside traditional healthcare settings
Consumer mobile apps provided information about COVID-19, tracked symptoms, provided home fitness programs
Patient receiving care at home

(IQVIA Institute, Jun 2021; Report: Digital health Trends 2021: Innovation, Evidence, Regulation, and Adoption. IQVIA Institute for Human Data Science, July 2021)

Digital potential and EU solutions

The digital framework highlights the most critical cross-border sustainable cost feasibility and minimises health inequalities (Barbabella et al., 2022). Digitisation easily connects people to healthcare professionals. Healthcare professionals will spend more time satisfying better ways of patients after gaining appropriate digitisation skills. Digitisation, which strengthens practice and aligns with local authorities, makes health systems more accessible and universal. It provides incentive growth and stimulates European industry. Yet health professionals and patients have doubts about Digital health system products, e-health, transparency data collection, and cost-effectiveness. However, the EU started the digitalisation of different forms of healthcare as a single digital market (European Union, 2020).

Changes due to the pandemic

The EU has tried to provide a rapid response to the pandemic, although it lacks the necessary competences to do so (Aristei et al., 2022). All member states are united under the umbrella of the European Union and are developing a framework that takes European Health Sovereignty into account. A single-window system thereby allows public and private cohesion policy regulated by the EU. Research and development to increase the production of innovative advanced Medicines and design robust healthcare infrastructure to minimise the impact of future pandemics while not compromising the European Health Standard. In addition, Germany, Portugal, and Slovenia, known as the Tripartite presidency in the EU council, come together by committing to the best resilient health systems in the world.

Under von der Leyen's Commission, an Expert Group on Health Systems Performance Assessment (SPA) was launched. This swears member states to a single slogan, which is an essential tool for sharing and staying together on a common agenda, health policy integration (Expert Group on Health Systems Performance Assessment, 2020). In addition, the Commission's EU Health Policy Platform team includes more than 7000 members to provide a stage for open discussion, critique, and debate on current policies.

As part of the digitisation of the healthcare, health-related data is to be exchanged quickly. The Trio's goal is open and loud to source healthcare legislation to give a strong voice, raise regulation, and provide sound updated release systems used in medicines and medical devices (Calvo Ramos & Economic and financial Committee, 2016). Furthermore, the Commission aims to bridge the digitisation gap among citizens by providing education. Further, the Commission has earmarked 9.4 billion euros to reshape the healthcare system over the next seven years. The EU also initiated the EU4th program, which aims to revitalise the entire health program and add new features apart from the standalone health programs. The new programme will be funded with an additional 413 million euros (Directorate-General for Health and Food Safety, 2022). This program provides a broader perspective on building advanced Healthcare products and systems capacity through a new research funding framework for 2021-2027 (Lupu & Tiganasu, 2022).

The digital future of the health system

Prevention is better than cure is an approach to better health that digitalisation promotes. We can say that the hour of failure and need triggered by the pandemic has highlighted the weakness of the health system (Martyna & Sascha, 2017), which is to be mitigated by digital solutions. In this context, the European Commission has established the European Health and Digital Executive Agency.

Europe is a health policy and research centre; The EU should facilitate multiple systems at different levels in 27 countries to explore health horizons. EU digitisation requires full-powered independent health technology assessment bodies to analyse health procedures and technologies. Digitisation promotes a flexible, primary model of care in the form of preventive care, mainly through investment in ICT information and communication technology.

The European Union has inspired the health sector globally to frame the priorities of the SDGs that focus on absolute health, and well-being policy should participate in every sector development program. Currently, 11,000 scientists from 150 countries have signed documents confirming the degradation of ecosystems and the extinction of species due to man. This document advocates a one-health approach for all living organisms. Global health has always been a political issue, but Corona has revealed the truth. The tripartite council recognises that global health is integral to EU policy and no longer covered by the philanthropy program. The EU is significantly interested in improvising the primary health systems of developing countries through urgent multilateral cooperation. The European Health Data Space (EHDS) will be built on the basis of strong data governance, data quality and interoperability (European Commission, 2022). It aims to promote greater exchange and access to different types of health data (electronic health records, genomics data, data from patient registries etc.). The EHDS could be the foundation for a truly integrated healthcare system in Europe (Greer et al., 2022). It is intended that the EHDS will ensure that all active stakeholders in the health sector are able to maintain an up-to-date electronic health record. The EHDS will enable predictive techniques, which will improve the efficiency of patient operational flow within hospitals. It will enable the development of new innovative treatments through the secondary use of data, as well as personalised and precision treatments addressing general and rare disease. Therefore, the EHDS framework will need to be developed and implemented with a pro-innovation approach (European Commission, 2022). In closing, the EHDS initiative should be an integral part of every healthcare professional's (HCP) training and professional development (PPD). The EHDS initiative should enable HCPs to "enable individuals and the system to be their own change agents" - according to the International Foundation for Integrated Care (IFCI).

It is time to believe an orchestrated shift towards integrated care holds the solution to the chronic disease pandemic. Now is the right time to rethink healthcare systems in Europe, using the momentum of the COVID-19 pandemic and the inevitable and accelerating digitalisation in health. The success of the digitisation of healthcare depends on ensuring accountability, privacy, and security.

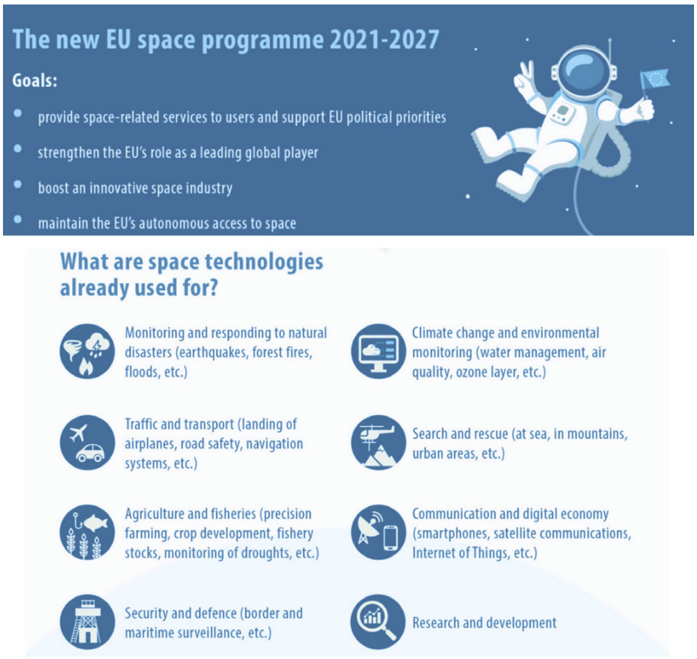
Abdul Ahad

ZEI Fellow, Master of European Studies, Class of 2022.

The EU in outer space

While Jean-Claude Juncker had claimed to lead a "political Commission", Ursula von der Leyen pledged to lead a "geopolitical Commission", which seeks to strengthen the EU's role as a global leader (European Parliament 2020). A great deal of political commentary has been devoted to the shift from "political" to "geopolitical." The prevailing view is that it signifies the EU's intention to assert itself as a global player in an increasingly hostile world. What much of the literature fails to consider is where the geographical limits of that world lie. Geopolitical literature tends to deal with the domains of earth, sea, sky and (increasingly) cyberspace (Douzet 2014). However, outer space is fast emerging as a territory in which global politics are played out (Doboš 2019).

From the very start of her tenure, Dr von der Leyen has treated the EU's space capacities as a priority. Her Commission included a new branch, DG Defence Industry and Space (DEFIS), which leads activities in the defence industry and space sector. In her Mission Letter to Vice President Josep Borrell, she stressed that the EU should be more strategic, assertive, and united in its approach to external relations and instructed him to "strengthen the Union's capacity to act autonomously" (von der Leyen 2019). Borrell's challenge resonates strongly in the space sector because progressing toward a more strategic, assertive, and united Europe in space is now essential to protect and promote European interests on the international scene (European Space Policy Institute 2019). Mr Borrell, who, incidentally, started his career as an aeronautical engineer at the School of Aeronautics and Space Engineering in Madrid, has repeatedly stressed the importance of space as a strategic domain. He has described space as "quite literally, the new frontier of global politics" (Borrell 2020a) and warned that the geopolitical tensions we see on Earth now extend and project into space (Borrell 2021).



The new EU space programme 2021-2027

Goals:

- provide space-related services to users and support EU political priorities
- strengthen the EU's role as a leading global player
- boost an innovative space industry
- maintain the EU's autonomous access to space

What are space technologies already used for?

- Monitoring and responding to natural disasters (earthquakes, forest fires, floods, etc.)
- Climate change and environmental monitoring (water management, air quality, ozone layer, etc.)
- Traffic and transport (landing of airplanes, road safety, navigation systems, etc.)
- Search and rescue (at sea, in mountains, urban areas, etc.)
- Agriculture and fisheries (precision farming, crop development, fishery stocks, monitoring of droughts, etc.)
- Communication and digital economy (smartphones, satellite communications, Internet of Things, etc.)
- Security and defence (border and maritime surveillance, etc.)
- Research and development

(European Union 2021)

Space is a strategic issue for the EU. Activities conducted in outer space are now critical to modern life on Earth (Nordman 2021). The mobile phones and online communications networks we now take for granted rely upon satellites in orbit. Those same satellites ensure that we can travel safely by land, sea, and air (European Space Agency). Space technology helps us monitor and improve the health of our planet. Infrastructure in space assists with emergency services, border management, agricultural sustainability, civil protection, and crisis management (European Parliament 2020). Space exploration pushes the boundaries of science and research. It also promotes and facilitates other policy areas such as security and defence, industry, and digital technology. The space industry creates jobs, boosts growth and investment in Europe, and is set to play a crucial role in the economic recovery after the COVID-19 crisis, in the EU's green and digital transitions, and in increasing Europe's strategic autonomy (Michel 2021).

The EU increasingly relies on space as a strategic domain to safeguard its economic prosperity, strategic interests, and security. However, space is becoming an increasingly challenging domain in which to operate. The threats and challenges are so grave Borrell has warned that the EU's freedom of access to and action in space is at stake (Borrell 2020b). The challenges have been termed "the three C's;" space is increasingly congested, contested, and competitive (United Nations 2021).

Space is congested. An increasing number of countries and actors are launching an ever-increasing number of satellites. Once the preserve of a few spacefaring nations, new states are making their presence felt in space. Some seventy-two countries now have space programmes, including India, Brazil, Japan, Canada, South Korea, and the UAE (Harding 2021). In addition, new commercial actors are entering the fold. Three of the world's richest men engaged in their own "space race" last year. One of them even managed to propel Captain Kirk beyond the stratosphere (Amos 2021). Beyond the egos and headlines, there is a serious point: an explosion of activity has increased the number of objects in orbit exponentially, and this looks set to continue.

The intensification of human activity in space has led to a proliferation of debris orbiting the Earth (European Commission 2020). As the amount of space debris increases, the risk of it colliding increases. Space debris poses a threat to the EU's space infrastructure, to the space services we rely on in our daily lives, and to our safety on earth - space debris poses a risk to ground-based infrastructures and citizens' security when it falls out of orbit and re-enters the Earth's atmosphere. Economic losses for European satellite operators stemming from collisions or collision avoidance are costly. Still, the real concern lies in the economic consequences "on the ground" due to the disruption of applications or services that rely on data from satellites lost or damaged (European Space Agency 2020). The greatest threat to satellites and space infrastructures today is the risk of collision with other satellites or space debris (Undseth, Jolly and Olivary 2020). The EU needs to protect its space-based assets and ensure the security of its ground infrastructure. The response should include enhanced space situational awareness capacities, cybersecurity and keeping pace with rapid technological developments. The EU should also be using its weight as a global player to help build the robust global governance essential to sustainable space activity (Michel 2021).

Competitive and contested: space is now vital for many sectors. It has therefore become a valuable resource. Increased competition over this limited resource increases the scope for contest and conflict. Space is increasingly a domain for great power competition, and this competition is increasingly taking on a military complexion (EUISS 2021). The USA recently created a formal Space Force as a sixth branch of the US military. Other states are following suit. NATO has adopted a space policy that recognises space as an arena for security competition (NATO 2021). Dr von der Leyen and Mr Borrell have expressed concern about the prospect of an arms race in space. Many space objects can be used for both civilian and military purposes. This makes them critically important to security and defence, but it can also make it difficult to discern the motives behind those who control them. Space is a territory in which irresponsible actions and threatening behaviours such as anti-satellite launches, proximity manoeuvres, jamming, dazzling and other displays of force are orchestrated by major powers (EUISS 2021). Borrell divides these threats and challenges into two pillars, which he envisages will form the foundations of the EU's future space policy. First, "security from space" is concerned with protecting the security of the Union and its citizens on Earth and second, "security of space" concerns the security of the Union in space, responding to threats to the Union's space assets (Borrell 2021).

In recent years the EU has taken several significant steps to progress Europe's space policy. It launched the new EU Space Programme in April 2021 and gave it a budget of 14,872 billion euros, the highest amount ever committed by Brussels for space programmes. In June 2021, the EU signed a partnership deal with the European Space Agency (ESA), which aims to deepen member states' investments in satellite navigation, Earth observation, space situational awareness, and secure communications. The EU allocated nearly €9 billion for the ESA and European industry to design new-generation systems and programmes for the period 2021-2027.

Despite these developments, many commentators believe that the EU is not sufficiently prepared to counter the threats and challenges it faces (see, for example, Fiott 2021). The European Defence Agency has stated that the EU's efforts are still too fragmented to be genuinely effective and recommended that the EU works to "develop a European approach to Defence in Space to improve access to space services and the protection of space-based assets" (EDA, CARD Report, summary, p.7). The proliferation of space-based activities we have seen in recent years is unlikely to abate. It is likely that traditional space powers such as the USA and Russia and newer space-faring nations such as India and Japan will increasingly use space to underpin their military power. If the EU does not act to both maintain and strengthen its presence in space, it will be exposed to greater risks both in space and on Earth. The Union has enjoyed great success in developing capabilities such as Galileo, EGNOS and Copernicus, and years of investment have ensured its autonomous space capacity today. However, Member States are still too fragmented in their strategic approach. The EU cannot afford to find itself unprepared to counter the weaponisation, congestion, and disruption that is taking place in space. Space is vital for the EU's way of life on earth. In the words of Josep Borrell, "While we fight the fires in our neighbourhood, we also need to shape the future. Protecting our security and economic interests in space is a strategic issue for Europe. Let's treat it as such." (Borrell 2020).

Caroline Frances Mair

ZEI Fellow, Master of European Studies, Class of 2022.

ZEI Master of European Studies

Welcome to our „Class of 2023"

Follow ZEI on Social Media

IMPRINT

ISSN: 2196-1409
Center for European Integration Studies
Genscherallee 3
53113 Bonn
Germany

Editor:

Henrik Suder
henrik.suder@uni-bonn.de

The Future of Europe Observer is published three times a year. Authors are responsible for the views expressed in their contributions. For references please contact the editors.

www.zei.uni-bonn.de