Working Paper
SWP Working Papers are online publications within the purview of the respective Research Division. Unlike SWP Research Papers and SWP Comments they are not reviewed by the Institute.

SWP

RESEARCH DIVISION EU / EUROPE | WP NR. 02, APRIL 2021

The Impact of the Digital Service Act (DSA) and Digital Markets Act (DMA) on European Integration Policy

Digital market regulation as one of five major digital policy projects of the EU [1]

Annegret Bendiek

[1] This paper was published as a written statement for the Franco-German expert discussion of the European Committee of the German Bundestag on 11 February 2021 (Committee document 19(21)135).

Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

Content

1 The Problem: Public Spaces in the Hands of Oligopolies

Europe has become the scene of intense political and economic struggles for its assertiveness in the digital world.[2] The omnipresence of US digital corporations, Europe's dependence on Chinese communication technology and Washington's influence on the boycott of Huawei's 5G technology emphasised Europe's heavy dependency on Asian hardware and US software products, particularly during the Covid-19 pandemic.[3] The EU's previous approach to multinationals in the digital economy is currently being fundamentally reconsidered. With a global market share of Google of about 80 percent of all search queries and a social media market share of 70 percent for Facebook and YouTube, we are in the midst of an unprecedented concentration process of the communicative infrastructures of democracy.

Given the increasing relevance of digital publics, communication in society is shifting towards a market-oriented realm where every expression of opinion comes at a price. Public digital discourse spaces are provided by private companies and access to them is controlled accordingly. Only those who enter into a private contractual relationship and make their contribution either monetarily or in the form of commercially usable data have a right of use or a say. Unconditional democratic participation tied only to citizen status is not provided for in these social networks developed for marketing purposes. This would be roughly comparable to a situation in which not only the parliament building is owned by a private provider and access to it is regulated according to economic criteria but also the volume of the loudspeakers and the transmission of speeches to the outside are evaluated according to the market. These risks to democracy have recently become clear with the blocking of @realTrump's Twitter and Facebook account.[4]

The Commission's antitrust proceedings against Google have been hanging in the balance for years, and the remedies in the Google Search (Shopping) case are considered unhelpful.[5] According to the dynamics of social networks effects, large platforms replace smaller ones, one can assume that the problem will also increase in other social areas (e.g. media streaming, digital education). The acquisition of WhatsApp by Facebook has already been approved by the EU Commission in 2014. Facebook was first and foremost a social network. Its own messenger service was well behind the ad-free and privacy-preserving WhatsApp. Meanwhile, Facebook has come to dominate the market for short message services. Contrary to the group, WhatsApp's contact and usage data was completely integrated into the

[2] This assertiveness can be understood as "digital" insofar as we are dealing with a comprehensive algorithmic recording and processing of facts in politics today. See in more detail: Armin Nassehi, *Muster: Theorie der digitalen Gesellschaft,* Munich: C.H. Beck Verlag, 2019.

[3] Florence Chédotal, "Thierry Breton, European Commissioner for the Internal Market: "Pour l'Europe, c'est la fin de la naivité", in: *L'Echo Républicain,* 25.1.2021.

[4] Cf. Christoph Schmutz/Daniel Steinvorth, "Die EU sagt der "digitalen Oligarchie" den Kampf an", in: *Neue Zürcher Zeitung*, 13.1.2021.

[5] Vgl. Dennis Brouwer, "A non-discrimination principle for rankings in app stores", in: *Internet Policy Review*, 9(2020)4; Dennis Brouwer, "Towards a ban of discriminatory rankings by digital gatekeepers? Reflections on the proposal for a Digital Market Act", in: *Internet Policy Review*, 11.1.2021.

Facebook ecosystem, and the opening for (election) advertising was implemented.[6] The EU's previous regulatory approaches, such as relying on voluntary commitments, failed to do justice to this concentration of power. The "Code of Practice" was assessed rather critically by civil society, academia, media and fact-checkers. Researchers found hundreds of thousands of Facebook comments calling for politically motivated violence only on Election Day in the US. In the context of the German "doxing affair" in December 2018/January 2019, the online platform Twitter was slow to react despite the Code's voluntary commitment. The storming of the Capitol in Washington in January 2021 is a "wake-up call" for Europe (High Representative Josep Borrell).

Due to the consequences of network effects, large platform providers hardly have to fear competition in Europe. The remaining remedy is thus either a fundamental reform of antitrust and competition law or merely a cautious further development of competition law. The previous antitrust procedures for assessing and controlling monopolies, such as the concept of "consumer harm", often fall short. The central problem often cited is that the big companies regularly buy burgeoning, smaller competitor start-ups from the market before they can become a threat to the business model (killer acquisitions). The purchase of WhatsApp and Instagram by Facebook are exemplary here. Efficient and certainly not fair competition no longer exists in many areas.

On 15 December, Vice-President Margarethe Vestager and Commissioner Thierry Breton published on behalf of the EU Commission two draft regulations to regulate digital services and digital markets, "which primarily target the gatekeepers of the internet"[7]: the Digital Service Act (DSA) and the Digital Markets Act (DMA). Much of the e-Commerce Directive is elevated to the rank of regulation. DSA and DMA are envisaged to introduce stronger accountability and due diligence obligations on digital services and digital markets to enforce transparency in the networks and make disinformation and agitation a risky business. As EU regulations, they would be directly applicable in the member states in the future. This regulatory package is being received very positively in the media, because with this reorganisation of the digital economy in Europe and worldwide, damage to democracy can be averted. [8] This is at least the overall goal.[9] The legislation is intended to redefine the digital economy's central rules and is by far not the only legislative package to come closer to this goal.

[6] During the presidential election last year, there was a ban on election advertising for the first time (with a time limit), see Oliver Bünte, "Facebook: Polit-Anzeigen für weiteren Monat ausgesetzt", in: *Heise Online*, 12.11.2020, < https://www.heise.de/news/Facebook-Polit-Anzeigen-fuer-weiteren-Monat-ausgesetzt-4957557.html>.

[7] Rupprecht Podszun/Sarah Langenstein, "Gatekeeper im Visier", in: *Legal Tribune Online,* 16.12.2020, <https://www.lto.de/recht/hintergruende/h/eu-digital-wirtschaft-regulierung-plattformen-intermediaere-dsa-dma-kommission-datenschutz-kartellrecht/>.

[8] Felix Karrte, "Resilient gegen Trump und Twitter. Die EU-Gesetzesinitiative zu Tech-Konzernen stärkt Grundrechte und Gesellschaften", in: *Der Tagesspiegel*, 13.1.2021, p. 6.

[9] Vgl. Guilaume Klossa, "Les médias, premier pilier de la souveraineté numérique de l'Europe face aux GAFA", in: *Le Figaro*, 1.12.2020; Agieszal Kumor, "Digital Act: l'Europe veut limiter la toute-puissance des geants du numerique", in: *RFI*, 15.12.2020; Jan Penfrat, "L'Europe a besoin delois qui limitent le pouvoir des grandes entreprises du numérique sur nos vies", in: *Le Monde*, 15.12.2020.

2 European Re-Sovereignisation: 5 Major Digital Policy Projects of the EU

Sovereignty must be rethought today.[10] It can neither stop at the outdated notion of popular sovereignty (la volontée générale), nor at the legal requirement of legal rule-making authority, nor at Carl Schmitt's pretence of ultimate power. Sovereignty today is more appropriately understood as a multi-level political practice in Europe. The EU has the delegated function of bringing together member states' public and private interests and providing them with appropriate liability and security provisions for the platform economy and social media in the relevant international standard-setting bodies. Corporate expertise must be brought together with consumer interests and ethical considerations in the overall European interest. This is beyond the scope of national governments.

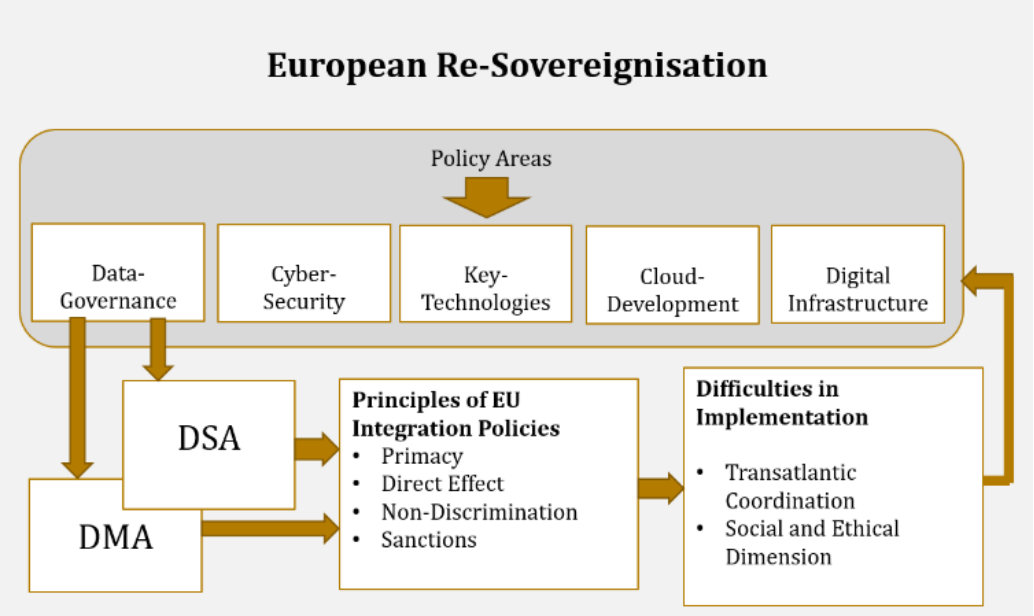
The globalisation of European data protection regulations, the promotion of rule-of-law oriented, precautionary technology governance in the area of artificial intelligence, cloud development such as GAIA-X, the Cybersecurity Act and its new certification requirements for hardware, software and also for digital network infrastructure such as 5G and the screening of foreign investments in key digital technologies are clear reactions that are to be realised in the current Commission under Commission President Ursula von der Leyen to create technological sovereignty. The German government had announced during its trio Council presidency the goal of making Europe "technologically and digitally sovereign". [11] 20 per cent of the funds of the Next Generation EU development programme are to flow into digital projects. [12]

The political goal is: The French Council Presidency in 2022 with the Conference on the Future of Europe will have to bring all measures of the five major digital policy projects to a successful conclusion with concrete results. In all these fields, it is not only about the economically motivated internationalisation of own standards but also about the maintenance of the European social model (*un nouveau contrat social*). The EU has lately recognised the problem: Market power is closely linked to political design. Facial recognition software, social scoring and other surveillance tools are already available on the European market for the control and suppression of dissidence. Chinese infrastructure implies the possibility of Chinese influence. Anglo-Saxon notions of limited data privacy are associated with US cloud and video conferencing providers. The battle for technological supremacy is thus also a "battle of narratives" (Josep Borrell), in which the European social model itself is up for grabs. In order to survive in this new environment, Europe must develop "digital sovereignty" and think like a geopolitical power.

[10] See also from a French perspective Guilaume Klossa, "as de souveraineté numérique pour l'Europe sans souveraineté médiatique", in: *Les Echos*, 29.12.2020.

[11] See also Ursula von der Leyen, *A Union that strives for more. My agenda for Europe. Political Guidelines for the next European Commission 2019-2024*, Brussels, 2019. "This is also a priority of our German EU Council Presidency. We need our own smart and ambitious European digital strategy with which we can consistently bring together foreign, economic and technology policy and create a strong, sovereign and innovative Europe", see Auswärtiges Amt, "Europa muss digitale Macht sein. Minister of State Michael Roth in the FAZ", Berlin, 4.10.2020, < https://www.auswaertiges-amt.de/de/newsroom/roth-faz/2402136>.

[12] Ursula von der Leyen, "Wir müssen die Macht der Internetkonzerne demokratisch einhegen", in: *Die Welt*, 28.1.2021.


European Re-Sovereignisation
Policy Areas
Data-Governance
Cyber-Security
Key-Technologies
Cloud-Development
Digital Infrastructure
DSA
DMA
Principles of EU Integration Policies
• Primacy
• Direct Effect
• Non-Discrimination
• Sanctions
Difficulties in Implementation
• Transatlantic Coordination
• Social and Ethical Dimension

3 DSA and DMA as a Sovereignty Project for EU Integration

Sovereigns entities are those who can bring together domestic private and public opinion-forming processes and articulate them in European and international bodies in such a way that the European model of society endures. While most agree on the aim of European sovereignty, most disagree to what extent internal market policies should be geared towards the goal of EU's digital sovereignty. The protest against upload filters has led Brussels to re-define the concept of EU digital sovereignty. The protests against upload filters have brought about "a change of heart in Brussels"[13], says Julia Reda. Digital sovereignty no longer refers merely to a legally defined state but must be related to the moderating capacity of EU actors, represented by the EU Commission and the Council of Ministers, to legitimise their positioning through transparent opinion-forming processes. The concept of digital sovereignty is analytically helpful, offering guidance for outlining the challenges of the digital transformation and the development of European capacity to act. Complex digital sovereignty is subject to a corporatist will-forming process and for this the EU Commission has launched a public consultation on the DSA from June 2020 until September 2020. These laws are subject to high lobbying pressure. According to Lobbycontrol, the top five companies with the highest lobby spending in Brussels include Google, Microsoft and Facebook. Coordination between the digital ministries and parliamentary committees as practiced on 11 February 2021 by a joint meeting of the European Affairs Committees of the Bundestag and the Assemblée Nationale presents a prerequisite for the decision-making process. It will take until 2022 for these regulations to enter into force. This political process is exemplary for other digital policy projects.

DSA and DMA are one building block of a total of five major digital policy projects of European re-sovereignisation (see Diagram: European re-sovereignisation). As a substructure, many individual regulations are already in force, ranging from consumer law to intellectual property law and the geoblocking regulation. In addition, there is "B2B platformisation" and "datafication" in the digital economy, which includes traditional industrial companies but are not the subject of the DSA (See below chart "Data"). The EU Commission presented its data governance initiative on 25.11.2020. The Data Act is to follow in 2021. However, competition and data protection law have so far been unable to curb the growing market power of corporations. With the legal acts DSA and DMA, political resources are being [14][15]concentrated supranationally under parliamentary co-decision, as with the implementation of the GDPR, in order to prevent the mere accumulation of too much data in

[13] Julia Reda, " Der Digital Service Act steht für einen Sinneswandel in Brüssel ", in: *Edit Policy*, 5.1.2021, <https://www.heise.de/hintergrund/Edit-Policy-Der-Digital-Services-Act-steht-fuer-einen-Sinneswandel-in-Bruessel-5002121.html>.

[14] Official Journal of the European Union, *Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for* business *users of online intermediary services (Text with EEA relevance)*, L 186/57, Brussels, 11.7.2019,

[15] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Law)*, COM(2020) 767 final, 2020/0340 (COD), Brussels, 25.11.2020.

one hand: "An anti-data dominance law that ensures the unbundling of too large data blocks - even if there is no demonstrable market abuse."[16]

3.1 DSA and DMA are complementary (positive and negative integration)

DSA-E and DMA-E are complementary to each other in order to avoid legal and content-related contradictions. Negative integration means that restrictions on free trade are removed. They have a market-creating effect. The DSA is thus intended to create uniform platform regulation throughout Europe, because unilateral efforts such as the German network DG increasingly hinder the European Single Market when online platforms have to comply with different, sometimes even contradictory, sets of rules. Liability and responsibilities of digital services are to be regulated more clearly and, above all, more uniformly throughout the European Union.

Positive integration on the other hand means using economic policy and regulatory powers at EU-level to overcome market failures. The reporting and deletion of illegal content is intended to avoid democratic policy risks and guarantee users' fundamental rights. However, the DSA also integrates negatively, as it establishes liability privileges. Similarly, the DMA serves on the one hand to combat excessive market power and on the other to establish positive behavioural obligations.

The DSA builds on the e-Commerce Directive (2000/31/EC), improving transparency and modernising consumer protection and content issues and finally extending the General Data Protection Regulation.[17] The DSA will apply a modern system of compliance cooperation (control and enforcement) to large platforms. Furthermore, the DMA takes a closer look at the so-called gatekeeper platforms in the run-up to a dominant market position in order to create a level playing field for the digital internal market. Here, EU law has effects even beyond its own market by interfering with the business models of the large international internet groups, at least if they specifically target people in the EU with their services. Due to the size of the internal market, the EU is not only an important place of regulation, but at the same time a strong economic actor with a global ambition for digital self-assertion, which can be accompanied by new conflicts in transatlantic data transfer. [18]

In the EU Parliament, this is linked to the ambition to "put the constitution of the internet on a modern basis". The declared aim of the DSA is to enable all people to exercise the rights guaranteed to them by the Charter of Fundamental Rights, in particular the right to freedom of expression and information, freedom to conduct a business and freedom from discrimination.[19] In Art. 1 of the DSA, the Commission defines its intention: The regulation is intended to harmonise the rules for intermediaries, i.e. online platforms that provide intermediary services, by regulating in particular exemptions from liability, special due diligence obligations for certain platform operators and enforcement. Chapter II of the draft defines liability issues for digital services. Chapter III of the DSA contains clearly outlined due diligence obligations that must be complied with. The Provider privilege should be

[16] Lucia Puttrich, "Wir können Google entflechten", in: *Frankfurter Allgemeine Zeitung*, 10.12.2020.

[17] See Laura Ziegler et al, " Digital Service Act (DSA) et Digital Markets Act (DMA): l'Europe vise une régulation équilibrée du Net", in: *Edition Multimédi*, No. 248, 25.1.2021.

[18] See Dan Clark, "US General Counsel are watching as EU prepares for new data privacy laws", in: *New York Law Journal,* 24.12.2020.

[19] See p.18 DSA(3): "Responsible and diligent behaviour by providers of intermediary services is essential for a safe, predictable and trusted online environment and for allowing Union citizens and other persons to exercise their fundamental rights guaranteed in the Charter of Fundamental Rights of the European Union ('Charter'), in particular the freedom of expression and information and the freedom to conduct a business, and the right to non-discrimination."

maintained. Upload filters are not to exist. Instead, notice-and-action rules for illegal content will be in place, like other requirements, for example on the suspension of user accounts or on transparency in advertising.[20] The draft regulations target large tech companies with at least 45 million monthly active users in the EU and a market capitalisation of 65 billion (Art. 25 para. 1, DSA, Art. 3 para. 2 lit b DMA) to limit their market power. Only one European group - the German software developer SAP - reaches this market size. The DMA-E is the Commission's answer to the EU's previous a de facto powerlessness vis-à-vis the infrastructure providers of the internet. According to Art. 1, the rules should ensure "contestable and fair markets" in the digital sector.

3.2 Platform Regulation according to the Principles of the Community of Law

The realignment of the European Digital Single Market goes far beyond a mere regulatory framework for the market. It touches on essential fundamental rights and is highly relevant for the character of the EU as a democratic and liberal order. Digital single market regulation must additionally take into account the conditions of international competition and the current system competition with China as well as the different transatlantic regulatory traditions. So far, European rules breathe the spirit of a time when Facebook was not even founded. The contemporary competition rules are from the founding period of the European project. The e-commerce directive was adopted in 2000.

An update regarding the principles of the legal community is consequently indisputable. In fact, the new legal bases reinforce the principles of the European community of law and are thus directly related to the effort to re-sovereignise the EU. These include the primacy and direct effect of European law, the principle of non-discrimination and binding sanction mechanisms.

3.2.1 Supremacy and Direct Effect

In the order of competences, European law takes precedence over national law. With the approval of the Council and the European Parliament of the two regulations, all their provisions become direct effect upon entry into force. Platforms will then no longer be able to rely only on national substantive law, but they must delete all content that contradicts European provisions.[21] This requirement is politically explosive. For example, it would oblige platforms to remove content from politicians if it contains blatant false claims, lies or hate speech, depending on the legal situation in the member states. Article 20 of the DSA requires a company such as Twitter[22] to "suspend" an account if a user "frequently provides manifestly illegal content". Article 21 requires online platforms to notify law enforcement authorities if they suspect "a serious criminal offence involving a threat to the life or safety of persons has taken place".

Consequently, Brussels would become a supervisory authority for the political space in the member states. In order to ensure the protection of users' fundamental rights, the DSA provides that the respective platform that removes content or suspends accounts must

[20] A concise summary is provided here by Podszun/Langenstein, "Gatekeeper im Visier" [as fn. 7].

[21] The DSA-E takes its place alongside a large number of provisions of EU law; moreover, it also does not completely supersede state law, especially with regard to substantive standards. See in more detail Prof. Dr. Martin Nettesheim, *Die unionsrechtliche Regulierung großer Internet-Plattformen. Die Kommissionentwürfe für einen Digital Market Act und einen Digital Service Act*, Written statement for the Franco-German expert discussion of the European Committee of the German Bundestag, Berlin, 11 February 2021.

[22] See Karrte, "Resilient gegen Trump und Twitter" [as fn. 8].

explain its action and set up a complaints system. The case can eventually be referred to an independent out-of-court appeal body. Moreover, the draft states that if security-related counter-terrorism ordinances exist, there should also be the possibility of upload filters in the future, even though the DSA excludes them. A new regulation is to oblige internet platforms to delete terrorist content in less than one hour after an official order. The draft regulation also assumes that all platforms are operated by commercial companies, however, non-commercial projects such as Wikipedia must also implement these rules. The Council and the European Parliament should therefore ensure that non-profit large companies are given special consideration.

The material scope of the DSA is not limited to political content. It also includes provisions for child pornography, terrorism or other criminal offences. The DSA must hence be understood as a "European NetDG", which is additionally extended by stricter regulations for advertising and a uniform handling of illegal content. Contrary to the demands of consumer protection groups, there is no general ban on microtargeting, i.e. personalised advertising and tracking. Nevertheless, the direct effect on companies strengthens transparency obligations for platforms and benefits consumer's interest: [23]

1. Hosting providers must justify their blocking decisions to users. Central databases are to publish which reasons are used for this. The EU has taken the Lumen database in the USA as a model for this in order to maintain transparency for journalism and scientific interests.
2. Online marketplaces must verify the identity of all traders and disclose it to consumers. Failure to disclose this information may result in marketplaces losing their liability privilege and being liable for product damage.
3. Platforms with more than 45 million monthly users in the EU must provide a public database of all advertisements served, including their reach and target groups. In addition, platforms are obligated to submit regular risk analyses in order to prevent phenomena such as election manipulation or disinformation campaigns. Consumers should be able to decide whether they want to be the addressee of recommendation algorithms.

In contrast to the DSA, the DMA stands in a comparatively liberal regulatory context. Its competence basis is not competition law exercised by the Commission but the internal market law. It is determined rather by the member states because several member states have concerns about ceding competences to Brussels in the control of large platforms.

Nevertheless, the DMA has bite.[24] Among the practices automatically prohibited and subject to fines is the merging of personal data from two services if this is done without the proper consent of the user, even if the same gatekeeper is behind it.[25] Companies should also be guaranteed the freedom of choice to offer their products or services on other platforms at different conditions. The EU should only intervene in the market if it is indispensable for the functioning of a free market. The DMA thus stands alongside European and national antitrust law without replacing them. This is to take into account the different market

[23] See in more detail Reda, " Der Digital Service Act steht für einen Sinneswandel in Brüssel" [see footnote 13].
[24] Also recommended " Das „Digital Services Act“-Paket - Europas Antwort auf die Macht der großen Tech-Konzerne?", in: *Noerr,* 22.12.2020, < https://www.noerr.com/de/newsroom/news/das-digital-services-act-paket>.
[25] A direct effect of EU law would be very interesting if the Facebook decision of the Federal Cartel Office is now uniformly regulated at EU level in the future. Accordingly, Facebook had to stop the aggregation of user data. Facebook was exploiting its market power by giving its users the choice of either accepting Facebook's terms of use and agreeing to the use of their external data or not being able to use Facebook at all (cf. BGH sets limits on Facebook's use of data). On the GWB, the German legal act, cf: Philipp Bongartz, "Happy New GWB!", in: *D'Kart Blog*, 14.1.2021, < https://www.d-kart.de/blog/2021/01/14/happy-new-gwb/>.

economy traditions of the member states. In political practice, however, it cannot be ruled out that the EU Commission will increasingly supplant the Federal Cartel Office and other national authorities.

It remains to be seen to what extent the regulatory package is compatible with the principle of data minimisation (Art. 5 para. 1 lit. C GDPR). Online platforms are to be obliged to provide comprehensive access to stored data. For example, researchers may be allowed to access archives in order to investigate disinformation and illegal advertising content. Uniform enforcement is challenging because current enforcement practices in data protection vary greatly in Germany, France and Ireland.

3.2.2 Non-discrimination

In the EU's internet governance, non-discrimination includes the prohibition of any illegitimate discrimination not only of public but also of private competitors.[26] In the DSA, all intermediaries that moderate user content are to make these moderation rules and the measures to enforce them public in their general terms and conditions in future.

This means that a recipe platform may in principle continue to prevent all uploads that do not refer to recipes. However, the company must disclose how it operationalises the term "recipe". Everything that can be subsumed under this term must then be treated equally ("non-discriminatory"). So far, the DSA is still unclear with regard to the question under which conditions platforms may highlight their own products. The same applies to preventing the uninstallation of software already installed at the time of purchase.
The DMA also contains an antitrust regulatory approach which the EU Commission already put up for discussion in June 2020.[27] Furthermore, the "New Competition Tool" includes the possibility of prior inspections of companies.[28] According to Art. 3 of the DMA, these can already take effect if there is an overriding interest in the "unbundling" of companies that provide "core platform services" without a breach of antitrust law having already been established.

The proposed legislation additionally stipulates that users should be allowed to uninstall pre-installed software applications (cf. Art. 6 para. 1 lit.b and c DMA): To enable end user choice, gatekeepers should not prevent end users from unstalling any preinstalled software applications on its core platform service and thereby favour their own software applications. Providers will also be obliged to allow alternative app stores. The implication of this regulation would be that app stores would no longer be permitted in their previous exclusive form, but would have to be opened to all providers, regardless of their contractual relationship with the respective platform.

In principle, DMA addresses all social networks, namely search engines, cloud services, video platforms, operating systems and advertising networks. However, the provisions are linked to exceptionally demanding criteria. These include significant influence on the domestic market, the role as a gateway intermediary, and a consolidated and lasting position, defined as 6.5 billion Euros in annual turnover or a market capitalisation of 65 billion Euros. Currently, these criteria would probably only be met by comparatively few US providers, while European start-up platforms would remain exempted. The regulations are intended to give the EU the possibility to take action ex ante against possible abuse.

[26] Non-discrimination means "comparable situations should not be treated differently and different situations should not be treated in the same way unless such treatment is objectively justified", in: *Open Internet Access Regulation*, recital 8.

[27] Cf. " Das „Digital Service Act“-Paket" [see fn. 24].

[28] Cf. European Commission, "Impact Assessment for a possible New Competition Tool. Policy field", <https://ec.europa.eu/competition/consultations/2020_new_comp_tool/index_en.html>.

3.2.3 Compliance and sanctions

Enforcement of the Regulation (regulated in Chapter IV, DSA) is in principle the responsibility of member state authorities. Collective redress mechanisms will only be activated if the above provisions are met. In order to implement the DSA, Member States shall appoint "Digital Services Coordinators" (Art. 38ff DSA), who are to monitor the enforcement of the EU requirements and ensure in a joint committee that the enforcement of the provisions is practised uniformly. At best, the member states must appoint a consumer protection officer. Failures can amount to fines. The amount is determined by the member state, but may not exceed the maximum amounts set by the Commission. The country where the intermediary has its headquarters is responsible. It is stipulated that the Commission should have the right to intervene in proceedings against large platforms by imposing fines itself.

In terms of sanctions, payments of up to six per cent of the total worldwide group annual turnover are possible in the DSA and up to 10 per cent in the DMA. In comparison, the GDPR (Art. 83) only allows fines of up to 4 percent of the group's annual turnover. In the final analysis, the DMA even provides for the exclusion of companies from the European market. In the event of a repeat offence, groups can also be forced to divest themselves of individual business areas.

In practice, the notice-and-take-down procedure, i.e. the procedure by which platforms collect information about possible illegal content on their services, is likely to become relevant. Hosting providers must have systems in place where users can report suspected illegal content. From a certain size of the business model, complaint procedures against illegal blocking must be provided. So far, the DSA does not sufficiently distinguish between different types of illegal content. Consumer advocates see the danger of reintroducing upload filters through the back door because the fully automatic blocking of content is allowed as long as the platform makes the use of such filter systems transparent.

4 Difficulties in Implementation

4.1 Transatlantic Conflict Potential

Questions of data regulation in the EU go far beyond the DSA-E and DMA-E. They affect the transfer of data between states and economic areas directly. The ECJ declared the Privacy Shield agreement on economic data transfer with the US invalid on 16 July.[29] However, the ruling has not only consequences for the approximately 6,000 companies that currently transfer their data to the USA under this Privacy Shield but also for all companies that work under the current EU standard contractual clauses (SCC) and transfer data to third countries. The EU Commission has provided previously valid model contracts for data transfers for this purpose. Consumer lawyers, litigation funders and legal-tech companies are drafting data protection complaints that, in their view, even the SIAs cannot provide an adequate legal basis for data transfers. If there are no solutions to the SIA, European and international companies will lose their legitimate business basis. Companies would have to stop their services, causing immense economic damage while intensifying the decoupling of economic areas and fragmenting the internet. Data transfers with Chinese service providers such as Bytedance, which have their headquarters in China and are subject to control by Chinese security authorities, pose in this regard an even greater challenge. Bytedance with the video platform TikTok does not pose a classic security threat, but it can be assumed that there is no complementarity with the GDPR and the European protection of children and young people. Bytedance TikTok uses facial recognition software and AI applications that are not allowed in the EU, pending a detailed review. The Irish Data Protection Authority was commissioned by TikTok in June 2020 to review the data processing and to present options. However, the Irish data protection authority feels it is out of its depth after Irish authorities had already taken action against Facebook.[30] It issued a request to no longer carry out data transfers in accordance with the standard contractual clauses. European data protection authorities are working on proposals for solutions. Three possible solutions are being discussed:

1. Adaptation of the standard contractual clauses (SCC): The EU Commission had intended to adapt the SCC in 2020 and develop a "broad toolbox" for data traffic. Here, data exporters and data importers must plausibly justify that data is processed in accordance with the General Data Protection Regulation (GDPR). For this purpose, *apropriate supplementary measures* to the SSV can be defined. Currently, companies make do with ad-hoc risk assessments, which are also documented. Part of such an assessment is the sensitivity of the transmitted data. Here, test criteria must be taken into account: Is the data interesting for foreign intelligence services? Can the encryption of data be enabled? SSV can be

[29] The ruling in the case "Data protection Commissioner v. Facebook Irleand and Maximiliian Schrems", 16.7.2020 (Case No. C-311/18); see also Björn Vollmuth, "Personal Data Transfer to the US and other non-EEA Countires", in: *Mondaq Business briefing*, 14.9.2020; Sven Venzke- Caprarese/Dennis-Kenji Kipker, "Neusortierung des internationalen Datentransfers", in: *Weser Kurier*, 1.9.2020; Commerce Department, "U.S. Surveillance Law Doesn't Threaten EU Privacy", in: *Cybersecurity Policy Report*, 28.9.2020.

[30] Cf. "Facebook's EU-US data transfer mechanismen 'cannot be used", in: *EurActiv*, 10.9.2020.

safeguarded by additional contractual regulations, by information obligations and special termination rights.

2. Transatlantic vote: Data protectionists like Maximilian Schrems argue that as long as the US Surveillance Act undermines the European Charter of Fundamental Rights, there is no solution. The Council of Europe and the Committee of Convention 109 Human Rights Organisation advocate an international treaty with safeguards. According to Reynders, Section Five of the Federal Trade Commission Act (FTCA), which is supposed to prevent unfair and deceptive trade barriers, is problematic. The change of administration in the US allows the use of Executive Orders to reform the Foreign Intelligence Surveillance Act (FIISA) and to appoint a Privacy Agreement Ombudsperson. It would enable the same level of data protection and the possibility of legal assistance of third-country nationals in the US and equal data protection provisions on both sides of the Atlantic. [31]
3. Data localisation in the EU: TikTok, Facebook are the push for European cloud development and thus for the European data infrastructure Gaia-X.[32] It is to operate as an international non-profit association under Belgian law. The 22 founding companies include Atos, Dt. Telekom, Bosch, SAP, etc. Participation requires acceptance of guidelines in line with European treaties. It promises an AI application that takes into account criteria such as data security, data protection or environmental sustainability. American and Chinese companies are welcome in the market but not in the Gaia-X initiative. Companies like Amazon Web Service appear as cloud providers in the Gaia-X demos, which raises questions of unequal treatment yet again.

With the Digital Service Act, the EU Commission is trying to give European data protection authorities a helping hand by creating a new supervisory authority for consumer protection. But not all EU states are pulling in the same direction: the European Court of Auditors warned on 10 September 2020 that bilateral agreements of 15 EU states with China under the Belt-and-Road Initiative violate European directives.

If Europe wants to become "technologically and digitally sovereign", the member states must support the EU Commission. New rules for the network are one thing. Creating European competitors is another. All five major digital policy projects are planned to be realised simultaneously. In spring, the Commission presents further important legal acts, for example for AI systems.[33]

4.2 The Social and Ethical Challenge

If member states try to use European digital and technology policy to reduce their own dependencies and change the 'balance of harm' in the direction of their opponents in order to open up greater room for manoeuvre for themselves,[34] they are potentially embarking on a path that has already proven disastrous in European politics. Rather than dismantling tech

[31] Brookings Institution holds Webinar on EU-US Privacy Shield, 10.9.2020, Political Transcript; see also Samuel Stolton, "Don't expect new EU-US data transfer deal anytime soon, Reynders says", in: *EurActiv*, 4.9.2020.
[32] See Timo Hoppe et al, "GAIA-X, Altmaiers Cloud wird europäisch", in: *Handelsblatt*, 23.9.2020; Catherine Stupp, "Europe's Cloud Project Mandates Security, Privacy Compliance" in: *The Wall Street Journal*, 8.6.2020.
[33] Christine Lambrecht, " Wehrhaft gegen Algorithmen. Auch KI muss Menschenrechte achten. Was die künftigen EU-Regeln zu leisten haben", in: *Der Tagesspiegel*, 18.12.2020.
[34] Cf. Mark Leonard/Jeremy Shapiro, *Strategic Sovereignty. How Europe Can Regain the Capacity To Act*, London: European Council on Foreign Relations (ECFR), 25.6.2019 (Policy Brief).

corporations, the goal should be a consciously designed "strategic" interdependence or openness as formulated by the EU Commission. An liberal understanding of digital sovereignty not only identifies endangered areas of strategic importance for Europe's services of general interest but at the same time also uses the opportunities of international division of labour within the framework of further deepened transnational networking, above all but not only with other large democracies. There must be an understanding "that European users and companies do not automatically benefit from limiting the power of large foreign tech corporations"[35].

Taking a Chinese perspective, globalisation in the digital constellation can only be stopped by authoritarian means and by compromising open societies. This authoritarian alternative to European re-sovereignisation is a relapse into international fragmentation and intra-European nation-state division. Both are incompatible with Europe's promise of "peace through integration" and would either lead to a technological dystopia or Europe's relapse into a digital and technological war of position. This cannot be an option for Europe. Sovereignty is complex and more of a process than a status. These legal acts will be crucial in determining whether liberal democracy and European integration will retain their credibility as proven instruments on the path to an inclusive welfare society in Europe. Their legitimacy depends on delivering not only innovation but also a solid measure of internal social stability and, at the same time, international openness. The internal unity necessary for this has at least two preconditions in Europe that are directly affected by digitalisation and can be described as the social and the ethical challenge of digitalisation. Data protection, content moderation, certification, ethical guidelines for the use of artificial intelligence and ecological and fair product standards are essential to keep the global development of sophisticated digital technologies in line with Europe's political values and cultural traditions. They are a necessary precondition to ensure social acceptance of a potentially disruptive technology. However, these regulations are not limited to Europe, but can also find imitators and gain validity worldwide.

The platform economy and associated rise of artificial intelligence (AI) signals a major transformation of capitalism with a significant potential for social dislocation. A study by the World Economic Forum (WEF) estimates that by 2025, work done by machines will increase from 29% to over 50%. Similarly, the McKinsey Global Institute estimates that about thirty to sixty percent of jobs can be fully automated. AI is increasingly learning to perform sophisticated intellectual tasks such as recognising complex patterns, synthesising information, drawing conclusions and making predictions, which not so long ago were thought to require human cognition. Such developments could be devastating for the political cohesion of member states. A society in which people become economically 'superfluous' quickly runs into difficulties in maintaining social cohesion. Technological innovations such as Blockchain and Virtual Reality (VR) could enable companies to evade regulatory authority at all levels of politics, deposit corporate profits in offshore havens, and circumvent democratic regulation as in the DSA and DMA. As a result, economic disparities in the EU are likely to increase and governments could lose the ability to organise redistribution would quickly lead to enormous political centrifugal forces within the EU. Normatively speaking: Only a social Europe will be able to maintain its capacity for internal unification.

[35] See the German original version: Jenni Thier, "Big Tech misstrauen – nicht dem Markt. Neue EU-Regeln für digitale Plattformen", in: *Neue Zürcher Zeitung*, 17.12.2020.

Dr Annegret Bendiek is Deputy Head of the Research Division EU/Europe.

SWP
Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

Ludwigkirchplatz 3–4
10719 Berlin
Telephone +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

doi: 10.18449/2021WP05