cerre Centre on Regulation in Europe

RECOMMENDATIONS PAPER

November 2020

Coordinated by
Alexandre de Streel

DIGITAL MARKETS ACT: MAKING ECONOMIC REGULATION OF PLATFORMS FIT FOR THE DIGITAL AGE

The CERRE recommendations are based on a series of four preparatory reflection papers and three workshops which took place in July and October 2020 with the following CERRE members: ARCEP, AGCOM, Amazon, Apple, BIPT, Comreg, ComCom, Deutsche Telekom, Facebook, Microsoft, OFCOM, Orange, Qualcomm, Spotify, Vodafone. During the workshops, these participating members made very useful comments and suggestions, including a number of views which have not necessarily been accepted by the authors. A non-attributable summary of these, as well as the preparatory reflection papers, will be published separately on the CERRE website.

The recommendations presented in this paper were prepared by a team of academics coordinated by CERRE co-academic director Alexandre de Streel and including Martin Cave, Richard Feasey, Jan Krämer, and Giorgio Monti. The academic team also benefited greatly from very useful comments by Amelia Fletcher.

As provided for in CERRE's by-laws and the procedural rules from its "Transparency & Independence Policy", this report has been prepared in strict academic independence. At all times during the development process, the research authors and the CERRE Co-Academic Directors and Director-General remain the sole decision-makers concerning all content in the report.

info@cerre.eu
www.cerre.eu

Table of contents

01

INTRODUCTION

1. Introduction

In its Digital Strategy Communication of February 2020,[1] the European Commission announced that the proposal of the Digital Services Act package would include one pillar aiming at achieving a fair and competitive economy through economic regulation. This pillar has now been renamed the **Digital Markets Act (DMA)**.[2] In their Inception Impact Assessment of June 2020, the Commission services indicate that they are considering the following three policy options: (1) revising the horizontal framework set in the Platform-to-Business Regulation;[3] (2) adopting a horizontal framework empowering regulators to collect information from large online platforms acting as gatekeepers; (3) adopting a new and flexible *ex ante* regulatory framework for large online platforms acting as gatekeepers which could be (3a) prohibition or restriction of certain unfair trading practices ("*blacklisted*" practices) and/or (3b) adoption of tailor-made remedies addressed on a case-by-case basis where necessary and justified.[4] In October 2020, the European Parliament adopted one resolution on the forthcoming Digital Services Act package with important directions for the Digital Markets Act pillar.[5]

This recommendations paper aims to contribute to this policy debate and is structured as follows: after this introduction, section 2 deals with the problems to be addressed and the recommended objectives for the DMA. Then, section 3 deals with the scope of the DMA, the criteria to designate Large Gatekeeper Platforms (LGPs), and the prohibitions and the obligations which may be imposed on those LGP. Finally, section 4 deals with the institutional design and the enforcement methods for an effective DMA. For several recommendations, the footnotes indicate existing best practices in EU law.

[1] Communication from the Commission of 19 February 2020, Shaping Europe's digital future, COM(2020) 67.
[2] There is now an understanding that the New Competition Tool may be integrated into the DMA and, therefore, could have a scope which is limited to the digital platforms. This paper is about the DMA and does not deal with the NCT as such.
[3] Regulation 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services, OJ [2019] L 186/55.
[4] Inception Impact Assessment on Digital Services Act package: Ex ante regulatory instrument for large online platforms with significant network effects acting as gate-keepers , available at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12418-Digital-Services-Act-package-ex-ante-regulatory-instrument-of-very-large-online-platforms-acting-as-gatekeepers
[5] European Parliament resolution of 20 October 2020 with recommendations to the Commission on the Digital Services Act: Improving the functioning of the Single Market (2020/2018(INL), in particular points 72-81 available at : https://www.europarl.europa.eu/doceo/document/TA-9-2020-10-20-TOC_EN.html

02

PROBLEMS AND OBJECTIVES

2. Problems and objectives

2.1. Main characteristics of the digital economy and possible need for intervention[6]

Although digital intermediation platforms are diverse in their business models, they are united by some **key features**: (i) important economies of scale and scope on the supply side; (ii) massive direct and indirect network effects on the demand-side; (iii) massive use of personal and non-personal data, (iv) high rate of innovation and importance of some key innovation capabilities; (v) uncertainty in the evolution of technology and markets; and often (vi) conglomerates that orchestrate entire ecosystems.

Some of those digital platforms may have a **gatekeeper function** when their consumers mostly single-home and have no – or little - ability or incentive to multi-home because, for instance, of lack of information, high switching costs, biases, and heuristics or lack of viable, adequate and competitive alternatives and there is a low risk of disintermediation. In this case, such a platform is the main bottleneck to this customer base and is in a position to leverage this gatekeeper position to its advantage. This may raise competitive and exclusionary issues when, for example, the platform providing intermediation services (i.e. services connecting business users and consumers or end-users) also competes with business users in their respective markets. This may also raise exploitative and fairness issues when the platform is using its bargaining powers to the detriment of the legitimate interests of its users.

However, the assessment of the economic effects of firms' conduct is particularly complex in the digital economy because specific **conduct often leads, at the same time, to pro and anti-competitive effects**.[7] For instance, the extension of a digital platform from one core market to another related market to offer a more complete suite of products and enlarge the ecosystem may benefit consumers, as such an extension increases the ecosystem's synergies. Such conglomerate diversification may also increase the economies of scope on the supply side. However, such an extension may lead to the exclusion of efficient niche competitors or discourage potential competitors from entering the market, thereby durably foreclosing the market or ecosystem. It may also lead to the exclusion of efficient providers of complementary products. Those examples show that assessing the competitive effects of conduct in digital markets often requires a difficult balancing of pro and anti-competitive effects. This is not specific to digital markets, but this is amplified in digital markets owing to the intensity of network effects and extreme returns on capital invested.

Therefore, assessing the economic effects of digital firms' conduct involves **several trade-offs** between different values, rights, and interests. Examples of those trade-offs are: (i) *short term and long term*: the conduct of a gatekeeper platform may increase consumer welfare in the short term, for instance by increasing short term competition or innovation, but at the expense of consumer welfare in the long term, for instance by reducing competition and thus harming incentives for good value and innovation; the most difficult situation occurs where there are clear short-run efficiency benefits and long-term competitive harm that is more uncertain but potentially very serious; (ii) *competition and innovation*: the conduct of a gatekeeper platform such as the acquisition of a start-up, may increase the development and/or the diffusion of the innovation of such start-up but at the expense of the competition that could have been brought by the start-up. To complicate the matter even further, trade-offs are also possible between different types of competition or different types of innovation. Arbitrating trade-offs is one of the main roles of regulatory agencies and the judiciary but such arbitration is particularly difficult in the digital economy because the trade-offs are amplified and have to be decided in a highly uncertain environment.

Given those difficulties, the **risks of errors**, of type I and type II, may also be amplified in the digital economy. Those risks can be decreased by reducing the information asymmetry between the digital firms and the public authorities and by increasing the learning curve of the authorities. This

[6] See the first issue paper for more developments.
[7] Digital platforms may also generate several positive and negative non-economic effect which are not analysed in this paper, although we recognize that they are important and may interact with the economic effects.

can be achieved with a better understanding of the digital economy through studies, market monitoring sector enquiries and market investigation, individual cases, as well as with information disclosure through appropriate rules and presumptions. The establishment of specialised and dedicated authorities may also contribute to reducing information asymmetry. Errors risks can also be reduced by doing a careful assessment of the effects of digital platforms conducts which take into account the diversity of the business models as well as the risks of regulatory failures and unintended consequences of public intervention on the functioning of the markets. Also, the **costs of type I and type II errors** may be amplified in the digital economy. The costs of type II errors could be decreased, in particular through timely intervention and swifter procedures when necessary.

2.2. Objectives of the Digital Markets Act

The DMA should have the following four main objectives:

1. Promoting **competition, market contestability and innovation**
2. **Empowering users**
3. Ensuring **fairness** in B2B relationships
4. Promoting the **Digital Single Market**

Based on the characteristics of the digital economy and the possible effects of the conducts of the Large Gatekeeper Platforms, we recommend the objectives of the DMA to be the following:

1. Promoting competition. The DMA should complement – and not substitute - competition law to promote competition, market contestability, and innovation when competition law is either ineffective or unable to intervene. Competition law may be ineffective because it is too slow or lacking the remedial measures necessary to preserve and restore the benefits of a competitive market to European consumers.[8] Competition law may also be unable to intervene in case of structural competition problems where the harm to competition is driven by underlying economic features of these markets more than by strategic firm conduct. Those structural problems include structural risks for competition when certain market features (such as network and scale effects, lack of multi-homing and lock-in effects) and the firms' conduct create a threat for competition. This applies to tipping markets, where the creation of powerful market players with an entrenched market and/or gatekeeper position needs to be prevented by early intervention or to unilateral strategies by non-dominant firms to monopolise a market through anti-competitive means.[9]

2. Empowering users. To foster competition, enhance innovation, and protect end-users' rights, the DMA should also provide users with relevant information and effective options to make informed choices. Reducing information asymmetries and giving users the tools and incentives to choose their preferred services could complement the ex-ante regulatory intervention and steer the market in the right direction.

3. Ensuring fairness in a B2B relationship.[10] The DMA should also protect business users and partners against the unfair practices of the gatekeeper platforms on which they depend. As already

[8] In the EECC, the insufficiency of competition law to adequately address market failures is one the three criteria justifying ex ante regulation: Directive 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code [hereinafter EECC], OJ [2018] L 321/36, art. 67(1). This third criterion has been clarified by the Commission in the following way: 'Competition law interventions are likely to be insufficient where for instance the compliance requirements of an intervention to redress persistent market failure(s) are extensive or where frequent and/or timely intervention is indispensable. Thus, *ex ante* regulation should be considered an appropriate complement to competition law when competition law alone would not adequately address persistent market failure(s) identified': Commission Recommendation 2014/710 of 9 October 2014 on relevant product and service markets within the electronic communications sector susceptible to *ex ante* regulation, OJ [2014] L 295/79, recital 16.

[9] See the Commission services' Inception Impact Assessment for the New Competition Tool: https://ec.europa.eu/info/law/better-rulation/have-your-say/initiatives/12416-New-competition-tool.

[10] In this sense, the DMA will complement the EU consumer protection law which ensures fairness in B2C relationship.

explained in the P2B Regulation, the large gatekeeper platforms "have superior bargaining power, which enables them to, in effect, behave unilaterally in a way that can be unfair and that can be harmful to the legitimate interests of their businesses users and, indirectly, also of consumers in the EU. For instance, they might unilaterally impose on business users practices which grossly deviate from good commercial conduct, or are contrary to good faith and fair dealing".[11]

4. Promoting the Digital Single Market. Finally, the DMA should ensure that the single market is not fragmented by a growing volume of national rules that regulate LGPs differently. Therefore, the DMA should promote the single market by imposing a common set of obligations on the LGPs and a common set of rights for the users of those platforms which should facilitate the scale-up of digital start-ups across the EU.

In achieving those objectives, enforcement action should comply with **good governance principles**, in particular the principles of proportionality, regulatory predictability and consistency, and respect for fundamental rights.

[11] P2B Regulation, recital 2.

03

SCOPE, CRITERIA FOR INTERVENTION AND PROHIBITIONS/ OBLIGATIONS

3. Scope, criteria for intervention and prohibitions/obligations

The scope of the DMA should **cover all online platforms** to be sufficiently flexible and future proof.

However, prohibitions and obligations should only be imposed on the online platforms which meet the following **four cumulative criteria**:

1. Be **large**, which could be measured by the number of unique users, time on site, or the proportion of interactions
2. Hold a **gatekeeper position** on which business users depend, which could be measured by the proportion of the large userbase with a low ability and/or incentive to multi-home or switch
3. This gatekeeper position is **enduring**, which can be measured by high entry barriers to both existing services and future services, because of the control of key innovation capabilities in the digital sector
4. Orchestrate an **ecosystem**, which implies a conglomerate presence

Those large digital gatekeeper platforms should be designated for a certain time by the EU body in charge of the DMA.

3.1. Scope of the Digital Markets Act

As the DMA intervention will be an asymmetric law, the scope of the DMA should be distinguished from the criteria to designate LGPs and which will trigger interventions. The scope determines the categories of digital platforms to which the designation criteria are applicable and not the platforms which will be regulated. In other words, the scope is necessarily broader than LGPs and not all platforms in scope should be regulated. The scope of the DMA should be broad enough to capture all types of digital platforms whose conducts *may* be harmful now and in the future.

Therefore, the scope of the P2B Regulation which covers certain types of online intermediation services[12] and online search engines[13] may be too narrow as it does not cover other digital platforms (such as operating systems or B2B marketplaces) whose conducts may potentially be harmful.[14] On that basis, we recommend that DMA **covers all types of digital intermediation platforms**. Following the OECD, this could be defined as "an information society service provider that facilitates

[12] P2B Regulation, art.2(2) defining online intermediation services as services which (i) constitute information society services; (ii) allow business users to offer goods or services to consumers, to facilitate direct transactions between those business users and consumers; and (iii) provide services to business users based on contractual relationships. Information Society Service is defined as 'any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient. The key elements in the definition are (i) the service must be provided for remuneration; (ii) at a distance; (iii) by electronic means; and (iv) at the individual request of the recipient of the service': Directive 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services [2015] OJ L241/1, art.1(1b).

[13] P2B Regulation, art 2(5) defining online search engine as a digital service that allows users to input queries in order to perform searches of, in principle, all websites, or all websites in a particular language, on the basis of a query on any subject in the form of a keyword, voice request, phrase or other input, and returns results in any format in which information related to the requested content can be found.

[14] The narrow scope of the P2B Regulation may be justified because it is a symmetric law whose obligations apply to all platforms in scope.

interactions between two or more distinct sets of users (whether businesses or individuals) who interact through the service via the Internet".[15]

3.2. Four Criteria to designate Large Gatekeeper Platforms[16]

The criteria to trigger regulatory intervention and designate the digital platforms on which remedies may be imposed should follow from the four objectives mentioned above. Besides, those criteria should be sufficiently flexible to adapt to different business models as well as technology and market evolution which evolve rapidly and can be unpredictable in the digital economy. The criteria should also be sufficiently clear and easy to implement to ensure legal predictability and not be subject to long and complex procedures.

Therefore, we think that the intervention should be based on the following four cumulative criteria, each of which should be assessed with quantitative and qualitative indicators. Those criteria should be assessed on a case-by-case basis during the designation process which should be done at regular intervals to take into account the rapid evolution of digital markets. The first criterion relates to the size of the platforms as the larger the platform is, the bigger the harm may be.[17] The three other criteria relate to specific features of platforms that make harm possible.

1. Size of the digital platform: this criterion may be determined based on the following quantitative indicators: worldwide and EU turnover,[18] worldwide and EU number of transactions mediated by the platforms, number of unique users in the EU,[19] time on site of those users.[20] Those indicators could be calculated as in absolute value (for instance, the number of users) or a relative value (for instance, the market share of users for a specific service such as search, online marketplace …). The advantage of absolute indicators is that they are easy to calculate as they do not require the definition of a relevant market or a business area. However, the disadvantage of absolute indicators is that they may not indicate the true economic power of the platforms as they are calculated independently of the size of the market or the business area.[21]

2. Gatekeeper position implying that users are dependent on the platforms: this criterion may be assessed based on a set of quantitative and qualitative indicators related to ability and the incentive of both sides of the market intermediated by the platform (i.e. the business users and the consumers) to multi-home on several platforms or to switch between different platforms as well as the ability and the incentive of the platform to prevent both sides of the market from going around the platform to deal with each other directly. Those indicators include the numbers of users who multi-home and the churn rate between platforms. The lower the incentive and ability to multi-home are, the more probable the finding of a gatekeeper position will be.[22]

---

[15] https://www.oecd.org/innovation/an-introduction-to-online-platforms-and-their-role-in-the-digital-transformation-53e5f593-en.htm

[16] See the third issue paper for more developments.

[17] An alternative option would be to designate gatekeeper platforms only on the three last criterion and rely on the platform size as a jurisdictional criterion to trigger the intervention of EU law (as opposed to national law).

[18] The Commission proposal for a digital service tax also relies on such indicator as it applies to digital platforms with total annual worldwide revenues of €750 million and EU revenues of €50 million: Commission Proposal of 21 March 2018 for a Council Directive on the common system of a digital services tax on revenues resulting from the provision of certain digital services, COM(2018) 148, art.4.

[19] The DSM Copyright Directive imposes additional stay-down obligations for content sharing platforms when the average number of *monthly unique visitors* exceeds 5 million, calculated on the basis of the previous calendar year: Directive 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market, OJ [2019] L 130/92, art.17(6). The EECC imposes on providers of number–independent interpersonal communications services the obligations to render their services interoperable if those providers reach a significant level of coverage and user up-take: EECC, art.61(2c). Some national laws on online content moderation also rely on users number as an intervention trigger.

[20] The EECC provides that Member States may impose reasonable 'must carry' obligations for the transmission of specified radio and television broadcast channels on the providers of electronic communications networks if a significant number of end–users of such networks and services use them as their principal means to receive radio and television broadcast channels: EECC, art.114(1).

[21] The concept of business area is used in the BEREC Response to the Public Consultations on the Digital Services Act Package and the New Competition Tool, BoR(20) 138.

[22] The EECC relies on a similar gatekeeper criteria to impose different types of obligations. It imposes on the providers of Conditional Access Systems (CAS) from which broadcasters depend to reach any group of potential viewers to offer to those broadcasters, on a FRAND basis, technical services enabling the broadcasters' digitally-transmitted services to be received by viewers: EECC, art.62(1) and Annex II, Part I.

3. Enduring gatekeeper position. This criterion, which relates to the strength of potential competition, may be assessed by the determination of two types of entry barriers:[23]

- First, the **entry barriers to existing services** will vary according to the business models of the digital platforms: an important entry barrier consists of cross-groups externalities and network effects which tend to be amplified by big data and AI technologies and increase with the development and the maturation of the markets.

- Second, **entry barriers to future services** that are related to the control of innovation capabilities; in the digital economy, those are data, key platforms elements, risky and patient capital, specific data, and computer skills.

4. Ecosystem orchestrator: this criterion may be assessed with the following indicators: presence in multiple markets or business areas which could be 'tightly' connected in the same vertical value chain or more 'loosely' connected, control of ecosystems as a web of interconnected and to a large degree interdependent economic activities carried out by different undertakings to supply one or more products or services which impact the same set of users.[24] According to this criterion, only the gatekeepers who are active in several connected markets and orchestrate an ecosystem could be subject to the prohibitions and the obligations of the DMA.

[23] The Commission gives the following examples of entry barriers: "economies of scale and scope, privileged access to essential inputs or natural resources, important technologies or an established distribution and sales network; other costs and other impediments, for instance resulting from network effects, faced by customers in switching to a new supplier.": Guidance of 3 December 2008 on the Commission's Enforcement Priorities in Applying Articles [102 TFUE] to Abusive Exclusionary Conduct by Dominant Undertakings, para.17.
[24] See the possible forthcoming reform of the Greek Competition law.

3.3. Prohibitions and obligations to be imposed on the Large Gatekeeper Platforms[25]

The following contractual terms and practices by large digital gatekeeper platforms should be **prohibited** to guarantee fair and competitive markets:

- Terms and practices which **dis-empower consumers to multi-home or switch**, such as default and nudges, anti-steering, limiting data portability.
- Terms and practices which **dis-empower business users to multi-home or switch**, such as Most Favoured National (MFN) or exclusivity clauses.
- Anticompetitive and **unfair leverage** of gatekeeper power across markets, such as specific types of self-preferencing and bundling.
- **Unfair contractual terms and practices**, such as retroactivity, termination/suspension.
- Given the multiple effects of terms and conducts in the digital economy, the large digital gatekeeper platform should have the **possibility to justify** its terms or practices with an efficient or objective defence. Thus, the prohibition amounts to a reversal of the burden of proof from the regulatory authority to the gatekeeper platforms.

Besides the large gatekeepers, platforms may be subject to the following **obligations** to guarantee market contestability:

- Provide **interoperability** to key services and access to key API.
- **Share** large volumes of **data** at the request of another firm for the benefit of users in general and which does not undermine good privacy practices.

Large Gatekeeper Platforms (LGPs) could be subject to two categories of intervention. The first category, which corresponds to option 3a of the Commission services Inception Impact Assessment, consists of prohibitions (negative obligations). Those prohibitions aim to ensure competitive and fair conduct on the markets for intermediation services. The second category, which corresponds to option 3b of the Inception Impact Assessment, consists of a variety of tailored remedies imposed on a case-by-case basis and enforced by a regulatory body. Those (positive) obligations aim to enable competition and stimulate contestability on the markets for the intermediation services. As explained in the following section, the prohibitions are easier to enforce than obligations that require a comprehensive governance framework. As the business models of the digital platforms are different, each category of intervention will have to be adapted to the specific business model of the LGP at hand.

[25] See the second issue paper for more developments.

3.3.1. Prohibitions to guarantee competitive and fair conducts

The first category of intervention consists of prohibiting certain conducts for which there is enough experience and certainty that they are harmful to consumer welfare, innovation, and business users' legitimate interests.

The list of prohibited conducts could be based on the following four types, which would need to be adapted to the type and the business model of the LGP:

- Practices which **dis-empower consumers** (one side of the intermediated market) by limiting their ability to multi-home on several platforms or to switch between platforms. This is, for instance, the case of default and nudges in choice architecture guiding users into making decisions that may not be in their best interests, anti-steering practice, or conduct that limit data portability.[26]

- Practices which **dis-empower business users and partners** (the other side of the intermediated market) by limiting their ability to multi-home on several platforms or to switch between platforms. This is, for instance, the case of Most Favoured Nation (MFN), non-competing, or exclusivity clauses.

- Practices which allow **anti-competitive and unfair leverage of gatekeeper power** across markets. This covers specific forms of harmful self-preferencing conduct, such as the unjustified use of business users' data.[27] This covers also specific forms of bundling detachable and non-necessary services.

- **Unfair** Contractual terms. The list of such practices could be built upon the list already contained in the P2B Regulation and include unilateral or retroactive changes to the contract, unjustified termination/suspension.[28]

As uncertainty remains high and harmful conducts can often also have positive effects and the business models of LGPs are diverse, it is recommended to leave the LGP the **possibility to justify its conduct** based on efficiency or objective justifications.[29] In practice, the LGPs should have the possibility to prove that its conduct is necessary and proportionate to achieve efficiency or other non-efficiency objectives such as the protection of the security or the integrity of the platforms.

3.3.2. Obligations to guarantee market contestability

The second category of intervention consists of imposing certain obligations to increase market contestability and facilitate the entry of digital platforms developing new services that can be a substitute or complementary to the ones already offered by LGP. In effect, those obligations will **open the platforms of LGP** to new entrants.[30] Such obligations could revolve around the following two types:

- **Interoperability and access to API** to enable complementary services to interwork with the core functions of the LGP (protocol interoperability) or to enable interworking between platforms that are substitutes to each other (full protocol interoperability) while maintaining the security and the integrity of the LGP.

[26] Beyond the limited data portability right provided by Regulation 2016/679 of the European Parliament and of the Council of [27] April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 (General Data Protection Regulation), OJ [2016] L 199/1, art.20.
[27] The prohibition of internal discrimination is also foreseen by several EU law: EECC, art.70 and Commission Recommendation 2013/466 of 11 September 2013 on consistent non-discrimination obligations and costing methodologies to promote competition and enhance the broadband investment environment , O.J. [2013] L 251/13; Regulation 80/2009 of the European Parliament and of the Council of 14 January 2009 on a Code of Conduct for computerised reservation systems and repealing Council Regulation 2299/89, OJ [2009] L35/49, arts.5,7,10.
[28] Also Directive 2019/633 of the European Parliament and of the Council of 17 April 2019 on unfair trading practices in business-to-business relationships in the agricultural and food supply chain, OJ [2019] L111/59, art.3.
[29] As it is the case in the draft 10th amendment of German competition law: Section 19a(2).
[30] Similarly, when the telecommunications sector was liberalized in Europe in the nineties, the deal was to maintain the vertical integration of the incumbent while forcing them to open their networks to competition with the Open Network Provisions (ONP): Telecom Liberalisation Green Paper, COM(1987) 290.

- **Data sharing** involving the bulk transfer of large volumes of data at the request of another firm for the benefit of users in general and which does not undermine good privacy practices and incentives for data minimisation. This obligation will apply asymmetrically to the LGPs only but horizontally to all sectors of the economy. Thus, this obligation is different from the existing data sharing obligation which tends to be imposed symmetrically but only in a sector-specific manner (such as payment services, automotive, or some network industries (energy, telecom, postal).[31]

Those obligations could be **very intrusive,** as they pose risks to incentives to invest and innovate and they are costly to implement by the LGPs. Therefore, they should be imposed:

- with great care, only when necessary to achieve market contestability;
- when they are proportionate to meet such objective;
- in a tailor-made manner, according to the business model of the LGP on which the obligations are imposed.

Enforcing those obligations will moreover be particularly complex. Enforcement will therefore require an effective and comprehensive governance framework, based on regulators having extensive expertise, information gathering and processing competence, and sanctioning power. It might be complemented by transparency or non-discriminatory obligations to ensure full effectiveness.

[31] In addition, the Commission is examining the need to impose more data sharing obligation in a forthcoming Data Act, which may apply symmetrically.

04

INSTITUTIONS AND ENFORCEMENT

4. Institutions and enforcement

Given the multinational presence of the large gatekeeper platforms, the DMA should mostly be **enforced at the EU level** either by the Commission or an ad-hoc body. Member State should also designate independent **National Digital Agencies to support** the work of the Commission or the EU body. All enforcement authorities should comply with due process and their decisions should be subject to a meaningful judicial review.

Given the characteristics of the digital economy, regulatory authorities should develop **New Ways of Enforcement** based on the following four principles: enforcement should be more **participatory, experimental, data-based, and technological.**

4.1. Institutional design[32]

As the LGPs are most of the time global and their conduct tends to affect the users in more than one Member State as well as the digital single market as a whole, we recommend the DMA to be **enforced at the EU level, either by the Commission[33] or by an ad-hoc EU body.[34]** The advantage of choosing the Commission is that a new authority would be costly and face a significant learning curve. Another advantage of choosing the Commission is that it will facilitate the coordination of DMA with competition law enforcement as the same authority will be in charge of both legal instruments at the EU level as well as with the other EU policies. The disadvantage is that the Commission is not an independent authority but plays an increasing political or geopolitical role. Another disadvantage is that the Commission may not have, at this stage, sufficient resources for this new role.

The tasks of the EU regulatory authority should be the following: (i) the designation of the LGPs based on the criteria and indicators mentioned above in section 3.2; (ii) the monitoring and the enforcement of prohibitions, possibly by giving more explanations of prohibitions to provide further guidance for LGP; (iii) the design, the monitoring and the enforcement of tailored-made obligations.

In enforcing the DMA, the EU authority should be supported and advised by national authorities which are closer to the consumers and the business users of the LGPs. Thus the DMA should also provide that each Member State designate a **National Digital Authority** with the standard features imposed by EU law on national regulatory authorities (in particular, expertise, independence, resources, information gathering, and sanctioning powers).[35] It will then be up to each Member State to designate such authority, which may be an existing one (for instance, the competition agency or the telecom regulator), a new one, or a national network between existing authorities. Such designation should build on (and respect) the recently introduced provision in the P2B Regulation to avoid inconsistent legislation

[32] See the fourth issue paper for more developments.
[33] As it is the case for the Code of Conduct for computerised reservation systems: CRS Regulation, arts.13-16.
[34] As it is the case for the systemic banks: Council Regulation 1024/2013 conferring specific tasks on the European Central Bank concerning policies relating to the prudential supervision of credit institutions [2013] OJ L287/63. The powers of the SSM are based on Article 127(6) TFEU. If the EU treaties do not provide for a specific legal basis, some claim, on the basis of the old *Meroni* doctrine, that the EU legislature cannot establish a new EU regulatory authority without a Treaty change as it would upset the institutional balance which gives executive powers to the Commission. However, the Court of Justice has recently validated the powers of the European Securities and Markets Authority (ESMA) which is tasked with direct supervision and enforcement against specific financial entities: Case C-270/12 *United Kingdom v. European Parliament and Council*, EU:C:2014:18.
[35] For instance, Directive 2019/1 of the European Parliament and of the Council of 11 December 2018 to empower the competition authorities of the Member States to be more effective enforcers and to ensure the proper functioning of the internal market, O.J. [2019] L 11/3, arts.4-12 ; GDPR, arts. 51-59; EECC arts.6-9.

The tasks of the National Digital Authorities could be the following: hear complaints from business users or consumers of the platforms and, when justified, forward them to the EU authority; monitor the enforcement of the DMA prohibitions in their national territory; advise the EU authority on the necessity, the proportionality, and the design of DMA obligations and, when appropriate, monitor the enforcement of those obligations in their national territory. Moreover, national authorities could particularly focus on purely national cases, while providing leeway for EU level action in cross-border cases.

Given the intrinsic European dimension of the platforms and to ensure effective action and advice by the National Digital Authorities, these should be **coordinated within a new EU network**. The design of such a network could be inspired by one of the following existing models: the European Competition Network (ECN),[36] the Consumer Protection Cooperation Network (CPC),[37] the European Data Protection Board (EDPB)[38] or the Body of European Regulators for Electronic Communications (BEREC).[39]

Given the great complexity of enforcing the regulation in the digital economy, the multiple and amplified trade-offs to be decided, it is key that all the authorities in charge of the DMA are sufficiently **independent** of the market players as well as of the political power. Authorities should also enjoy sufficient sanctioning power and impose **sanctions** that are effective, proportionate, and dissuasive when the prohibitions or the obligations imposed on LGPs are violated.

It is also key that the investigations, the procedures, and the actions of those authorities respect the fundamental rights which are guaranteed by the **Charter of Fundamental Rights of the EU** and that the perceived need for speedy action does not reduce the guarantee of due process and procedural fairness protected by the Charter. Moreover, given the still limited understanding of the digital markets and the risks of errors, it is also key that the decisions of the regulatory authorities can be subject to **review by an independent Court** which has access to the relevant expertise to assess the very complex trade-offs which are to be arbitrated in the digital economy. To be meaningful, such a legal review should take the merits of the case into account.[40]

4.2. New ways of enforcement

Given the characteristics of the digital economy, in particular, the amplified trade-offs to be arbitrated, the rapid and often unpredictable innovation, and the large information asymmetry between the LGP and the regulatory authorities, new ways of enforcement need to be found for the DMA to be effective and not remain a piece of paper in the official journal of the EU. We think that those new ways of enforcement should be based on the four principles described below.

First, enforcement needs to be **participatory** while being mindful of the risks of regulatory capture. This means that all stakeholders (i.e., the LGPs, their actual and potential competitors, their business users, and the consumers) should be closely involved in the implementation of the new rules. This should be particularly the case for the design of positive obligations aimed at increasing market contestability. The participation of the LGPs may be achieved by relying more on commitments.[41] However, this should not necessarily rely on self-regulation - which is often self-serving - in the case of gatekeeper power.[42]

Second, enforcement needs to be **more experimental** while remaining predictable. Given the novelty of many issues, regulators are bound to make mistakes but should minimise those. One way

[36] Regulation 1/2003, arts.11-13.
[37] Regulation 2017/2394 of the European Parliament and of the Council of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws and repealing Regulation 2006/2004, OJ [2017] L 345/1.
[38] GDPR, art.68-76.
[39] Regulation 2018/1971 of the European Parliament and of the Council of 11 December 2018 establishing the Body of the European Regulators for Electronic Communications, OJ [2018] L 321/1.
[40] See for instance, EECC, art.31.
[41] As used in competition law (Council Regulation 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty, O.J. [2003] L 1/1, as amended, art.9) or in telecommunications regulation (EECC, art.79).
[42] This is why the concept of Code of conducts, which often refers to self-regulation, should be alleviated in the DMA.

to minimise errors is to learn from experience. Evaluation should be done ex ante by running A/B testing of different types and design of remedies as the LGPs are now used to do before launching new services. Evaluation should also be done ex post by assessing the relevance, effectiveness, and efficiency of the remedies after some time of implementation.[43]

Third, enforcement needs to be **data-based**. As the LGPs themselves, the regulatory authorities should seize the opportunities brought by big data analytics and AI to increase the efficiency of their regulatory operations. This implies that authorities need to have extensive power to collect information from the LGP but also from their business users and customers (which corresponds to option 2 on the Inception Impact Assessment). Authorities also need to have efficient means and technologies to process that information with AI tools (data-driven regulatory intervention, Suptech and Regtech).

Fourth, when appropriate and possible, enforcement needs to be **by design.** This implies that the legal prohibitions and obligations should be as much as possible integrated into the technological design used by the LGPs and that the technical architecture should include, as much as possible, the rules themselves.[44] As put by Lessig, the legislative code should move to the computer code.

[43] On ex post regulatory evaluation: Commission Staff Working Document of 7 July 2017, Better Regulation Guidelines, SWD(2017)350, Chapter VI.

[44] See the privacy by design rule imposed by GDPR, art.25(1): Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

cerre

Centre on Regulation in Europe

Avenue Louise, 475 (box 10)
1050 Brussels, Belgium

+32 2 230 83 60

info@cerre.eu

cerre.eu

@CERRE_ThinkTank