

(Meta)verse as the Next Escaper from Competition Public Enforcement*

*Luca Megale***

ABSTRACT: While authorities discovered the need to regulate competition in the digital world, one of the Big Techs – Facebook – changed its name in Meta. The latter emphasizes the shift from being a social network company to becoming a metaverse one. The paper argues that a new digital world is laying its foundations, and competition public enforcement risks being caught off-guard again. Such a new world is based on the concepts of metaverse, web3 and the tools of algorithms and blockchain. The common element is decentralization; however, in the hand of a few main characters governing the sector as it is today – not the users. Therefore, public competition enforcement will have today's criticalities, yet heavily amplified by the characteristics of the metaverse. The paper addresses the potential impact of the metaverse on competition; starting from the essential facility doctrine, the application of its elements to the metaverse can only be hypothesized. However, it is noted that, in a worst-case scenario, the requirements would be met with some amendments (given by the nature of the new market). Moving on, it is asserted as tacit collusion might be a crucial issue due to algorithms and blockchain.

Metaverse might also be characterized by repeating concerns. Regulators' lack of attention on M&A review had a crucial role in the development of the present digital markets. The latter was the consequence of regulators not understanding the potential future outcome of acquisitions and impact on markets. This might already be happening again. Lastly, the metaverse could not only increase the data gathered by undertakings, but also their quality, thanks to the use of new technologies. Thus, amplifying

* Date of Reception: 13 May 2022. Date of Acceptance: 20 July 2022.

DOI: <https://doi.org/10.34632/mclawreview.2022.11715>.

** University of Rome LUMSA. PhD Student. Department of Law, Economics, Politics and Modern Languages, Faculty of Law. The author acknowledges the support of Tim S.p.A. through the PhD scholarship. ORCID ID: 0000-0002-8034-958.

the ability of predicting consumers' behaviour and undertakings' market power (to be added to the already present concerns on data exploitation).

To front this scenario, competition public enforcement, as it is today, might not be enough. The paper claims that a regulatory intervention is needed to avoid history repeating itself: while regulators have no clear idea on what and how to regulate the digital platforms, Big Techs continue their power climbing. In a still unknown metaverse infrastructure, what is needed is a future-oriented analysis of the problem drivers and scenarios.

Therefore, the proposed approach varies based on the specific antitrust concern. The common word is regulatory foresight; however, it must also be considered that a lack of uniformity between Countries – even EU Member States –, and the current hard adaptability of antitrust norms and doctrines (e.g., essential facilities), risk to hamper a needed regulatory adaptability.

KEYWORDS: Metaverse, public enforcement, regulatory foresight, Big Techs, megatrends

1. Introduction

Imagine going to work, then leaving the office, meeting someone in a café and shopping. A weekend off? Why not go to the Vatican Museum? However, you never left home. You are in the metaverse. Indeed, you visited the Vatican Museum by living in Chicago. While such a parallel virtual world will probably bring important innovations and potential benefits, new risks of regulatory enforcement failure are high. The latter with relevant effects on competition, a concern which regulators and enforcers already have a relevant struggle to curb. Margrethe Vestager recently stated “the metaverse will present new markets and a range of different businesses. There will be a marketplace where someone may have a dominant position” and “we should start thinking about it now”¹. Until now, the norm has been the so-called pacing problem, which specifically refers to the notion that technological innovation is increasingly outpacing the ability of laws and regulations to keep up.

¹ Samuel Stolton, “Vestager: Metaverse poses new competition challenges”, 2022, <https://www.politico.eu/article/metaverse-new-competition-challenges-margrethe-vestager/>.

The research questions of this contribution are 1) what effects the development of this new digital ecosystem may have and 2) whether current antitrust laws can work regarding the metaverse.

The paper argues that the metaverse development will amplify the already relevant issues for competition public enforcement in digital markets. The approach used (trying for many years *ex-post* regulating undertakings, which in the meantime reached a never-seen-before impact on society) needs to be reviewed. On this basis, the paper introduces the concept of the metaverse: decentralization controlled by users. While not disputing the merits of decentralization (e.g., tackling inequality and information asymmetry), the potential outcome might be the same that affected the initial ideas behind the creation of internet and social networks. In particular, there might be a power shift, but eventually the risk is to always have a few main characters governing the sector – not the users (par. 2). In view of this potential development of the metaverse, the impact on antitrust is imagined and analysed, focusing on the applicability of the essential facility doctrine elements to the metaverse; the risk of collusion through algorithms and blockchain; M&A review issues repeating; and amplified data exploitation concerns (par. 3).

After stressing the need for regulatory intervention, the paper argues that the way to go is to follow a strategic foresight approach. Moreover, regulatory agility and international co-operation must be assured to apply different approaches based on the specific situation. Indeed, the paper also tries to propose some regulatory interventions to the presented antitrust concerns, to safeguard competition and public enforcement (par. 5).

It must be made explicit that neither the author, nor anyone, can understand (to date) the impact of the metaverse on competition law. Nor can anyone understand the effectiveness of *ex ante* or *ex post* regulation or which laws or regulatory tools will be needed. Therefore, the aim can be no more than to hypothesize and introduce a discussion on the topic, and to follow the evolution of the matter with a future-proof and adaptive approach.

2. Non-decentralization of the Metaverse

The word “metaverse” comes from the Greek “meta” (μετα-), which indicates “beyond” or “after”, combined with “-verse”, as “universe”². The

² “Definitions, meanings, & Spanish translations”, *Lexico Dictionaries* | English, <https://www.lexico.com/>.

metaverse is a virtual reality with subtle boundaries between digital environments and the physical world. In such a parallel world, people will interact with virtual objects in real life, with real-time information and tangible impact in the world. Due to the increasing attention to the above-described word, it is now widely known that the term was coined by Neal Stephenson in the sci-fi novel “Snow Crash”³. The latter is set in a world in which humans interact through avatars in a three-dimensional virtual space⁴. The concept drifted from deep fiction towards science through the years; thus, becoming a hot-topic discussion.

Indeed, the digital world is a developing business environment and metaverse is the next chapter. A world in which we can completely live through our digital identity and avatar. This resurrected term, also thanks to the change in name from Facebook to Meta⁵, reflects the idea of an immersive experience that creates a mirror image of the real world in a digital one. Also, a combination between virtual and real-world, and the building of a new form of social interactions in the digital economic ecosystem. For instance, Zuckerberg posted a video of a haptic glove able to let people feel the pressure and texture of virtual objects⁶. The same video shows Zuckerberg using the product to play chess, in line with the CEO’s definition of a “platform even more immersive – an embodied internet where you’re in the experience, not just looking at it. We call this the metaverse, and it will touch every product we build”⁷. The idea behind the concept is that, linked to web3⁸ – and thanks to blockchain⁹ –, the metaverse will

³ Neal Stephenson, *Snow Crash* (Milano, Rizzoli, 2007), 24.

⁴ Alanah Davis et al., “Avatars, people, and virtual worlds: Foundations for research in Metaverses”, *Journal of the Association for Information Systems* 10, no. 2 (2009): 90-117, <https://doi.org/10.17705/1jais.00183>.

⁵ Introducing Meta: A social technology company (2021), in Facebook.com: <https://about.fb.com/news/2021/10/facebook-company-is-now-meta/>.

⁶ “Watch Mark Zuckerberg play Jenga and Fist-Bump in virtual reality using ‘haptic gloves’ that Facebook, now Meta, is building to let people feel objects in the Metaverse”, *Yahoo! News*, <https://news.yahoo.com/watch-mark-zuckerberg-play-jenga-234930754.html>.

⁷ Mark Zuckerberg, *Founder’s letter*, 2021, <https://about.fb.com/news/2021/10/founders-letter/>.

⁸ Another term, or better, concept – web3 – is broadly discussed along with metaverse. It is frequently used as a synonym of the metaverse, but it is not. It refers to a decentralized web, i.e., a different way of operating the Internet in client/server structure (in which data is managed and stored by trusted central entities), which would be replaced by blockchain technology (a distributed ledger on a peer-to-peer network) and a set of new protocols. Metaverse and web3 are considered deeply linked and represent together the highly decentralized future of the Internet.

⁹ The blockchain, made famous by the crypto world, like the Ethereum case, is based on a series of nodes. Each node keeps a copy of the distributed ledger that contains all transactions made by

belong to its users, not to a single undertaking. Thus, changing the way in which data is managed, taking power away from central governing structures, since it would be stored in multiple copies on a peer-to-peer computer network¹⁰; management rules would be formalized in protocols and guaranteed by the consensus of network participants, incentivized with a token for their activity.

Therefore, a virtual world governed by a decentralized community (with users that control their data and identity). The latter was actually the primitive concept behind the internet. However, from a network of networks, the internet is today a network of platforms¹¹. Besides, the metaverse will also change consumers' buying relation with companies and the market as a whole. Online social networks were defined as a new social environment that people create within a virtual world¹². If we interpret social networks as the place in which virtual platforms allow individuals to create their virtual public life, and companies to develop products or services (with a continuous communication between the two), the metaverse could be seen as a highly immersive social network. It has to be added that social media platforms are not designed for the direct purchase of products, but to redirect consumers towards e-commerce.

The metaverse will probably get those two above-mentioned worlds as close as possible. In social network platforms, the first step was to gather users' interest in a service able to deeply maximize the social interaction between people¹³. This phase of the business model led to reaching the critical mass, next to a constantly increasing network effect: new users

a given application, as in the case of a metaverse based on its technology. The registry is based on a sequence of blocks that cannot be modified. Any attempt to alter it would change the cryptographic code that binds one block with the next, effectively invalidating the entire blockchain. All this generates trust in the users since the safety of transactions is part of the whole idea behind blockchain.

Ethereum's blockchain has become the foundation for dozens of primitive metaverses and the technological basis for a massive variety of applications, ranging from financial to real estate.

¹⁰ "Bitcoin: A peer-to-peer electronic cash system", <https://bitcoin.org/bitcoin.pdf>.

¹¹ Julie E. Colen, "Between truth and power", 2019, <https://doi.org/10.1093/oso/9780190246693.001.0001>.

¹² Gregory Thomas Stafford, *Analysis of Social Networks in a Virtual World*. Theses and Dissertations. 925. <http://scholarworks.uark.edu/etd/925>.

¹³ Christopher J. Westland. "Critical mass and willingness to pay for social networks", *Electronic Commerce Research and Applications* 9, no. 1 (2010): 6-19, <https://doi.org/10.1016/j.elerap.2009.05.003>.

increasing the value of the service¹⁴. However, along with network effects, congestion is a potential outcome¹⁵. Indeed, the presence of too many people on the network led, in Europe, to reduced bit rates for videos on Facebook and Instagram¹⁶. Moreover, another shade of the congestion is the incredibly grown number of ads and companies and understanding of the business model by consumers, leading to the decrease of interest and much more difficulty on users targeting.

Given the above, the idea of Facebook might be to create a next-level social network, in which businesses will change their approach – bringing it closer to the real world. For instance, Nike will not need to result in the homepage of a user or employ an influencer as an intermediary to target the audience of interest. A company will have the chance to acquire a virtual shop in the busiest road of the metaverse. Additionally, the visualized shops may also change depending on the specific users' needs. Indeed, the physical interaction between users and businesses, being the face-to-face one¹⁷, will be present in the metaverse.

The concepts of centralization or decentralization apply to both physical and virtual networks, due to “virtual” being a reflection of the “physical” one. The idea of a decentralized network has been considered as an alternative social, economic and political structure¹⁸. The latter is able to tackle inequality and information asymmetry¹⁹. The main differences between decentralized and centralized networks are that the first one has no single point of failure (it is not possible to attack the central node and stop the functioning of the whole structure). There is no central authority control

¹⁴ The success of redesigning the relation between users and businesses was inevitable through ads and businesses' growing presence in the same social network, which allowed to reach an incredible amount of profiler users to target.

¹⁵ Michael Quinn Patton. “Process use as a usefulness”, *New Directions for Evaluation* 116 (2007): 110, <https://doi.org/10.1002/ev.246p>.

¹⁶ Foo Yun Chee, “Facebook to cut video streaming quality in virus-hit Europe”, *Reuters*, March 22, 2020, <https://www.reuters.com/article/us-health-coronavirus-facebook-idUSKBN2190VH>.

¹⁷ Face-to-face interaction is critical to cities: “(...) cities themselves are networks and existence, growth, and decline of urban agglomeration [and] depend to a large extent on these interactions” (Helsey, R. W.; Zenou, Y., (2011)). Thus, in the metaverse, one of the few elements that differentiate social networks and e-commerce from real shops will be added: local human capital externalities in civic participation.

¹⁸ Andrej Zwitter et al., “Decentralized network governance: Blockchain technology and the future of regulation”, *Frontiers in Blockchain* 3 (2020), <https://doi.org/10.3389/fbloc.2020.00012>.

¹⁹ Jaya Klara Brekke, “Hacker-engineers and their economies: The political economy of decentralised networks and ‘cryptoeconomics’”, *New Political Economy* 26, no. 4 (2020): 646-659, <https://doi.org/10.1080/13563467.2020.1806223>.

and gatekeepers, and thus censorship is more complex due to the decentralization of the information distribution²⁰. At the same time, the lack of a central authority raises coordination issues. Besides, the lack of censorship allows less possibility of supervision on the contents, and requires a particularly more complex organization and structure. To give an example of decentralization, the idea behind bitcoin is (or at least, was) to shift control from banks and intermediaries, giving rise to independent agents that communicate in an ideal competitive market. Participants cannot unilaterally alter the rules, and there are no exit network costs associated²¹.

However, some factors are not to be underestimated. Market participants are inclined to become monopolists, or at least to outsmart their competitors²². This leads back to centralization. Indeed, in the case of harmonized rules, each partner would have an incentive to deviate from what was agreed upon²³. Without central administration instruments set up, hubs might conspire, individuals might deceive one another, markets could be manipulated, and there could be a massive expense to individuals entering and leaving markets. In a parity situation, each participant would be inclined to “cheat” to increase its benefits and assume a monopolist position²⁴.

Lastly, and for what strictly concerns this paper, blockchain and distributed ledger technologies have led to the “re-thinking” and experimentation of old economic ideas, namely those concerning the organization and funding of distributed network, motivated by anti-authoritarian ideologies across the political spectrum²⁵. The latter leading to a virtual world based on the economic concepts of organizing commons and bonding curves²⁶. However, social and economic decentralization require the autonomous individual or rational economic agent to be willing and able to participate.

²⁰ Nathan Schneider, “Decentralization: An incomplete ambition”, *Journal of Cultural Economy* 12, no. 4 (2019): 265-285, <https://doi.org/10.1080/17530350.2019.1589553>.

²¹ For instance, Hayek conceived markets as an “information processor”, a decentralized mechanism to coordinate resources and needs.

²² Richard McKenzie et al., “In defense of monopoly”, 2008, *The University of Michigan Press*, <https://doi.org/10.3998/mpub.93419>.

²³ Pheidon Nicolaides, “A theory of regulatory integration”, *Intereconomics* 41, no. 1 (2006), 37-43, <https://doi.org/10.1007/s10272-006-0170-y>.

²⁴ *Ibidem*.

²⁵ *Ibidem*.

²⁶ *Ibidem*, 32.

Interestingly, the participants' expenses being in a decentralized world are generally high, while the advantages can be heavily restricted²⁷.

The improvement of information and communication technologies has updated our skills to pass on and exchange our information on an overall scale. However, users deal with internet through centralized platforms and services due to the combination of market dynamics and network effects that have led to a concentration of market power in a few operators. The virtual server structure has resulted in undertakings like Amazon, Facebook, and Google to establish highly centralized virtual networks of communications or e-commerce. Those have led to a shift from the idea of the Internet as a decentralized world to the already known result of a centralized structure, governed by some leading participants.

The idea of blockchain-based applications has led to hypothetical game conventions and market-driven motivations that really intensify – instead of disturbing – existing elements of capitalism and speculation²⁸. Indeed, blockchain is decentralized in data management or can be in data sharing, but not necessarily imply decentralization in the organization/infrastructure that uses it. Apparently, both the Internet and the consequent innovations are repeating patterns that result in a new set of incumbents that operate as the previous ones.

The metaverse clashing against the market (which will lead to the development of dominant participants and therefore centralization) will make such concept fail, as other decentralized-based concepts have done in the past – more famously, the Internet. However, the lack of centralization does not delete the potential existence of the metaverse. The latter will exist even without the planned decentralized organizational structure. In one scenario, if the infrastructure providers act solely as supervisors – it is difficult to imagine that Facebook will leave the business model characterizing its social network empire. In another one, leading undertakings will act as users' exploiters in exchange for the offering of unique and essential services for everyday life, as it is today. Indeed, the metaverse existence implies that more data will be produced and collected through an entire ecosystem built as a lab for companies seeking to increase the

²⁷ Rémy Prud'Homme, "The dangers of decentralization", *The World Bank Research Observer* 10, no. 2 (1995), 201-220, <http://www.jstor.org/stable/3986582>.

²⁸ Michael Casey et al, "The impact of blockchain technology on finance: A catalyst for change", *Geneva Reports on the World Economy*, 2019, <https://www.sipotra.it/wp-content/uploads/2018/07/The-Impact-of-Blockchain-Technology-on-Finance-A-Catalyst-for-Change.pdf>.

number of ads people click through – more than 95% of the Meta’s revenues come from ads²⁹.

Besides, in the already existing primitive metaverses, there is a continuous and incredible amount of money spent on virtual lands³⁰. Meta could be potentially interested in becoming the landlord or the real estate agency, placing ads in front of the street or taking a percentage on the ads placed on the brought house. For instance, inspired by YouTube, which provides a space for YouTubers to publish videos and takes a rate on the ads placed at the beginning, middle or end of the video. Some argue that it will not be possible to have a unique metaverse dominated by, for instance, only Facebook. Even today’s Internet is not centralized by an individual undertaking, but a few dominant ones. If this could be considered decentralization (probably not), it will be – but not in the hands of users. Meta announcing the Horizon platform seems to already go in such a direction³¹.

3. Antitrust concerns

Having discussed the potential metaverse development, it is crucial to analyse how it will actually impact the antitrust environment. The rise of digital markets has played a major role in the antitrust landscape. The focus points have mainly been the digital advertising and social networking markets.

While regulators and policymakers have finally put such issues at the top of their agendas, the digital economy with its main characters is already moving in a new direction.

As mentioned in the introduction, as there are still primitive traces of the development of the metaverse, the author can only attempt an analysis that sheds light on the most relevant issues. The choice of the specific issues analysed (essential facility doctrine, collusion, M&A, data exploitation) is simply a result of those contexts (within antitrust) in which the metaverse might have an impact, and in which there is already an interest of the relevant actors (e.g., Meta in M&A).

²⁹ See Facebook Q1/2021 earnings: <https://investor.fb.com/investor-events/event-details/2021/Facebook-Q1-2021-Earnings-/default.aspx>.

³⁰ Debra Kamin, “Investors snap up Metaverse real estate in a virtual land boom”, *The New York Times*, November 30, 2021, <https://www.nytimes.com/2021/11/30/business/metaverse-real-estate.html>.

³¹ See Horizon World Community: <https://www.oculus.com/facebook-horizon/community/>.

As widely known, the first step for an antitrust analysis is defining the relevant market. Simplifying, the relevant market is the one that is affected by the regulatory initiative. It comprises all products/services that are considered to be interchangeable or substitutable because of their characteristics, prices and use. In the metaverse, there would be two potential outcomes. One is considering the metaverse infrastructure as a relevant market itself (at least in the first phase). The latter, if there were more than one undertaking trying to provide the infrastructures behind the metaverse. The second one is considering different relevant markets inside the metaverse. For instance, the luxury sector undertakings selling clothes for the avatars; renting of budlings for smart working (which could also be the relevant market of the infrastructure provider, e.g., Meta); or the providers of the third-party objects to be used in the metaverse (e.g., a haptic glove).

Differently, the area in which the undertakings are involved in the supply (in a similar conditions' context) is defined as the relevant geographic market. Geographic market definition should serve two functions: facilitating an initial screen by allowing the construction of market shares, and, more importantly, reflecting the economic model of competition by identifying the core players within the market, who may reasonably be expected to constrain the competitive behaviour³². The easiest way to identify market shares and the core players reflecting the economic model would probably be to consider the whole metaverse as the relevant geographic market area. The latter, particularly if the same commercial conditions would be applied to all metaverse subjects. Indeed, the metaverse might be the representation of today's society, but without boundaries – even digital ones.

Over the paragraphs that follow, the analysis focuses on the essential facilities doctrine applied to the metaverse, the impact on collusion, the typical M&A concerns, and data exploitation.

3.1. Essential facilities doctrine

One of the companies that have been most under the spotlight is the already mentioned Meta. As stated, it is difficult, and it would be naïve to imagine that Meta will abandon its social media power and not move it into the metaverse. In today's internet interaction, a server connects with another server or an end-user device on a need-to-know basis. On the Internet,

³² Amelia Fletcher et al., *Geographic Market Definition in European Commission Merger Control: A Study for DG competition*, https://ec.europa.eu/competition/publications/reports/study_gmd.pdf.

simultaneous interactions are mimicked, but they are essentially different instances separated by fractions of seconds that people do not perceive³³. The metaverse will probably be as simultaneous video/social interactions, in terms of user experience and engagement; thus, the accomplishment will need to be based on an infrastructure.

In a potential scenario, Meta and other players could aim to become the undertaking providing the infrastructure and the underlying platform on which the metaverse could be based. The imagination could thus be oriented versus the doctrine of the so-called essential facilities. The latter is applied³⁴ to both tangible and intangible goods³⁵, where a refusal by an undertaking to comply with the above may be relevant under Article 102 TFEU, or Section 2 of the Sherman Act – concerning both the abuse of dominant positions. This refers to a total refusal to supply the goods or services and the imposition of barriers to entry that are so onerous as to result in a *de facto* denial³⁶.

Case law³⁷ among US and EU provides some crucial elements to define a facility as essential. Analysing the requirements by excess, an infrastructure should have the following characteristics to be considered an essential facility:

- (1) the (unjustified) refusal prevented the emergence of a new product, which the dominant firm did not offer and for which there was potential consumer demand;
- (2) a competitor's inability practically or reasonably to duplicate the essential facility;
- (3) the refusal allowed the dominant firm to reserve for itself the secondary market by excluding all competition on that market;

³³ "The Metaverse: The evolution of a universal digital platform", *Global law firm | Norton Rose Fulbright*, <https://www.nortonrosefulbright.com/en/knowledge/publications/5cd471a1/the-metaverse-the-evolution-of-a-universal-digital-platform>.

³⁴ The prerequisites for the application of this doctrine are: (i) the existence of a resource exclusively controlled by a dominant undertaking in a downstream market; (ii) the impossibility for competitors to duplicate the resource; (iii) the refusal of access by the dominant undertaking or conditions equivalent to such a refusal.

³⁵ EU Commission, "Magill", *Radio Telefis Eireann and Independent Television Publications Ltd v. Commission*, C-241 – C-242/91; EU Commission, *B&I Line/Sealink Harbours*, COMP. IV/34.689 (1993); EU Commission, *Telekomunikacja Polska*, COMP. 39. 525 (2011); EU Commission, *ENI*, COMP. 39.315 (2010).

³⁶ EU Commission, *Polaroid v. SSI Europe* (1984), paragraph 95; EU Commission, *Napier Brown/ British Sugar*, M. 30.178, paragraph 61.

³⁷ Magill (1995), Bronner (1998), IMS Health (2005) and Microsoft (2007).

- (4) the denial of the use of the facility to a competitor; and
- (5) the feasibility of providing the facility to competitors.

Indeed, to safeguard the incentive to innovate, the possession of monopoly power is not found to be unlawful, unless it is accompanied by elements of anticompetitive conduct. Since the topic deals with an infrastructure that does not yet exist, the analysis should focus on whether the nature of a metaverse might lead to the rise of an essential facility for its potential characteristics. It is a matter of fact that the current use of the internet, without Big Tech platforms being involved, is almost non-existent. Platforms leverage their exclusive control over search engines, ecommerce platforms, and app-stores, while the essential facilities doctrine has been either abandoned or considered not applicable to the new digital environment. The above in light of the trust in self-correcting markets and the willingness to ensure innovation.

The essential facilities doctrine elements application that follows is clearly hypothesized considering the worst scenario to be avoided.

- (1) The (unjustified) refusal prevented the emergence of a new product, which the dominant firm did not offer and for which there was potential consumer demand.

In the digital sphere it is not enough to consider “a new product, which the dominant firm did not offer”. This would lead to exclude the relevant concern of third-party products that competitors want to introduce in the market. For instance, consider the already mentioned example of the haptic glove. Meta would have a great interest in limiting the interoperability of another undertaking’s glove. The latter would not be a new product; thus, the requirement would not be applicable. However, consumers might want to use another undertaking’s haptic glove. For instance, because it includes additional features, or since it is customized in a marketing collaboration with another famous brand. Therefore, there would be consumer demand.

On a secondary basis, the same concept of the haptic glove or VR glasses might be applied to internal tools of the metaverse as, for instance, cloud&data hosting providers, or the suitability for payment processors (e.g., PayPal or also Coinbase), or famous communities creating avatars and 3D contents (e.g., Tafi) that would be competitors, for instance, to a Meta’s avatars marketplace.

(2) A competitor's inability to practically or reasonably duplicate the essential facility.

In the case of one infrastructure providing the metaverse, several factors might contribute to a competitor's inability to duplicate a metaverse infrastructure (i.e., enormous concentration and gatekeeping power) led by one of today's Big Techs. For instance, network effects given by the disproportionate value added by additional marginal connections and transactions the metaverse platform might enable. Thus, entry barriers derived from such network effects might pose a high risk of protecting the infrastructure provider from rising competitors and easily exclude them.

Besides, such network effects and high level of market concentration normally have led to markets having one main leading character³⁸. Additionally, the digital platforms era has shown users tend to "single home", meaning that they prefer living in one ecosystem. This might be extremely amplified in a metaverse characterized by exclusive agreements with working places, public offices for the issuing of certificates, agreements with sport association for the broadcasting of matches, and so on. The latter are examples of why a consumer would not have incentives to change ecosystem.

Therefore, the inability for a competitor to duplicate the essential facility would be the result of the strong network effects of the infrastructure and the unique links between the infrastructure and external elements/services.

(3) The refusal has allowed the dominant firm to reserve the secondary market for itself by excluding all competition from that market

Digital platforms operate with varying degrees of integration. The boundaries between providing general or specific service are limited. For instance, Google Maps nowadays provides reviews on restaurant or services showed in its maps (vs TripAdvisor and other competitors); Apple controls IOS, which could be essential to competition in the IOS app distribution market. For instance, Meta's Oculus has an app store that charges a fee for purchases made in the apps. Therefore, the metaverse provider will have a direct or indirect impact on an undefined number of secondary markets³⁹. This element will play a central role in defining an anticompeti-

³⁸ Martín-Laborda et al., "Merger control and online platforms: The relevance of network effects", *Market and Competition Law Review* I, no. 2 (2017), 78-85.

³⁹ It is easy to link this to the Epic Games and Apple well known case.

tive conduct by an undertaking. However, attention has to be put in identifying the relevant market. Indeed, a metaverse infrastructure reflecting the physical market would potentially give to the provider the possibility to limit (to itself) all existing market segments.

(4) The denial of the use of the facility to a competitor.

On such a point, the applicability to the metaverse could be linked to a proposal to deal on unreasonable terms. Indeed, it would be naïve to imagine a direct deny the use of the facility. On the opposite, proposing unreasonable terms is already allegedly happening on the app stores' market. As already mentioned, the assumed metaverse is a virtual reality platform that comprises both the social networking and e-commerce life. Besides, a source of profit would easily be in-app (in-metaverse) purchases. Therefore, the applicability of this requirement might be found in the metaverse.

(5) The feasibility of providing the facility to competitors.

It is clearly not possible to tackle this requirement in the present situation. However, this element often leads to the inapplicability of the doctrine. In particular, because of the need to show evidences of the feasibility of facilities added to the easy-to-be-found justifications of the facility owners. For instance, economic loss, ability to serve its own customers or impossibility given by designed characteristics of the infrastructure. Therefore, to solve the issue beforehand, cooperation between regulators and the big players would be crucial for the development of an infrastructure that is designed to assure competitors' access. It is true that the technological revolution of the past years – based on progress made in communications, connectivity, digitalization – has improved the quality of life. However, it has also meant the rise of a huge power of various business groups. A power that goes beyond ordinary and often proves to be stronger and more pervasive than the one of Governments⁴⁰. Indeed, market power often gets translated into political one⁴¹. And such market power – not only economic – gives space to inequalities. The latter, mainly thanks to the behaviour of large companies that gather, process, and use data on age, gender, residence, household, food, commercial, cultural preferences, spending power. As of today, this already requires a sophisticated technological structure that

⁴⁰ Marco d'Alberti, "Concorrenza e giustizia sociale", in *Mercato Concorrenza Regole* 2/2020, doi: 10.1434/98662.

⁴¹ *Ibidem*.

competitors are unlikely to be able to deploy, representing a formidable barrier to entry into these markets capable of excluding undertakings from competition (which are trying to make the moats broader and wider). It might be too soon to understand which undertaking, if, and how, would be able to reach such a position and to exploit it, contrary to the provision of art. 102 TFEU. However, the latter does not mean that boundaries could not be set in advance.

3.2. Collusion

The goal is to foresee and support the development of a metaverse based on a competitive cooperation between undertakings and interoperability between services proposed by different undertakings that will compose the metaverse. Encouraging a global and interoperable metaverse (with clear and numerous pro-competitive potentialities) – and multiple companies to co-operate – might lead to sharing competitively sensitive information or agreeing on pricing. Big Techs already communicate between them. For instance, Facebook and Google allegedly signed a deal that guaranteed Facebook would both participate and win in a fixed percentage of Google's online ad auctions⁴². Thus, regulators and enforcers should be put in the position to understand what is happening outside but, more difficultly and importantly, inside the metaverse. Tacit collusion, in which each participant might reach the anticompetitive outcome in benefiting from collective market power without explicit communication, should not be underestimated⁴³. As well as algorithms – which will be the foundation of the metaverse – educated to collude should not be belittled⁴⁴. The possibility of algorithms capable of setting prices in an autonomous way, or algorithms capable of reacting and adapting prices based on competitors' ones, is not

⁴² Martin Coulter, "Mark Zuckerberg and Sundar Pichai personally oversaw an illegal deal that misled publishers and advertisers, unredacted suit alleges", *Business Insider*, January 17, 2022, <https://www.businessinsider.com/google-and-facebook-execs-allegedly-signed-off-illegal-ads-deal-2022-1?r=US&IR=T>.

⁴³ OECD, *Algorithms and Collusion: Competition Policy in the Digital Age*, <http://www.oecd.org/competition/algorithms-collusion-competition-policy-in-the-digital-age.htm>; Joseph E. Harrington Jr, "A theory of tacit collusion", *Economics Working Paper Archive* 588, The Johns Hopkins University, Dept. of Economics, <https://ideas.repec.org/p/jhu/papers/588.html>.

⁴⁴ Ariel Ezrachi et al., "Sustainable and unchallenged algorithmic tacit collusion", *Northwestern Journal of Technology & Intellectual Property* 17, no. 2, 40.

new⁴⁵. This could lead to an extreme virtual world based on algorithms, facilitating collusion in a market prone to coordination⁴⁶.

Schrepel has already tackled the issue of algorithmic collusion, yet considering it a non-fundamental issue⁴⁷. However, such a line of thought could lead to underestimating an issue that might already exist (lack of empirical evidence could be the result of authorities not looking for it) and be amplified in the future. Then, it is still unclear who should be deemed liable. Generally, we could hypothesize two types of algorithms working inside the metaverse. The first one is algorithms playing against each other. Each undertaking has its own algorithm. The algorithms set the prices based on the market data environment. Following the price setting, the algorithms observe the actual market behaviour (for instance, the prices set by the competitor) and gradually stabilize the price. Another possibility is for undertakings to agree with the infrastructure provider in setting a unique algorithm that equals the prices between a given range. In both cases the issue lies in the detection of the collusion by competition authorities. Therefore, if the concern to be solved regards competition authorities' detections tools and their powers, specific regulatory intervention is needed to tackle such issue (par. 5).

As an additional element to take into account, Schrepel diverts the attention to blockchain-based collusion⁴⁸. Not underestimating algorithmic collusion, blockchain-based one could also be pivotal in the metaverse. Some of the potential outcomes would be decentralized agreements, or data sharing (on pricing), difficult to find. Besides, unknown identity of its participants (pseudonymity) and relative impossibility to enter, alter, or stop such agreements based on the blockchain⁴⁹. Thus, the nature of the blockchain would lead to have protected communications between undertakings with very low detection risks. Schrepel addresses as colluders may use a blockchain to share the price of their products⁵⁰. He also focuses on various types of

⁴⁵ *Ibidem*.

⁴⁶ CMA, *Working paper. Economic working paper on the use of algorithms to facilitate collusion and personalized pricing*, paragraphs 5.35-5.37, 2018, 14.

⁴⁷ See Thibault Schrepel, "The fundamental unimportance of algorithmic collusion for antitrust law", <https://jolt.law.harvard.edu/digest/the-fundamental-unimportance-of-algorithmic-collusion-for-antitrust-law>.

⁴⁸ *Ibidem*.

⁴⁹ See Thibault Schrepel, *Blockchain + Antitrust: The Decentralization Formula*. Cheltenham, UK: Edward Elgar Publishing Limited, 2021.

⁵⁰ *Ibidem*.

blockchains, since some of them are more likely to induce collusive agreements⁵¹. This is nothing utopic. There are already some cases of blockchain-related cases. For instance, the famous *Gallagher v. Bitcointalk.org*⁵², and the recent *In re Tether v. Bitfinex Crypto Asset Litigation*⁵³.

The same issue is reflected in smart contracts⁵⁴. While those could facilitate security, transparency, and lead to more efficient transactions and decreasing costs, they could give rise to collusive conduct by giving undertakings the tool to enter and maintain a cartel. Besides, by also assessing the behaviour of collusive partners. For instance, introducing the condition of withdrawing money if a partner deviates from the agreed conduct. Additionally, smart contracts could automate transfers between colluders and make side payments⁵⁵. Therefore, communication via blockchain should also be addressed in the needed regulatory intervention (par. 5).

3.3. M&A review

Concerning M&A review in the metaverse, there are no new elements. Just the same old story related to the non-attention of authorities to new rising markets, and the differentiated approach between States, which leads to a lack of harmonized intervention. M&As play a key role in shaping the structure of the digital market. Indeed, a firm can grow by increasing the sales of its products in the market and by merging or acquiring control of another one⁵⁶. From a market point of view, the question is whether a merger reduces competition by distorting the market through post-merger price increases, or by practicing unfavourable conditions to counterparties.

However, not all mergers are examined by the authorities. In fact, they need to be notified only when they reach certain turnover thresholds⁵⁷,

⁵¹ Thibault Schrepel, "Collusion by blockchain and smart contracts", *Harvard Journal of Law & Technology* 33, no. 1, 30.

⁵² See Schrepel Thibault, "The first case of 'blockchain antitrust': *Gallagher v. Bitcointalk.org*", <https://leconcurrentialiste.com/first-case-blockchain-antitrust/>.

⁵³ *In re Tether & Bitfinex Crypto Asset Litig.*, 19 Civ. 9236 (KPF) (S.D.N.Y. Dec. 20, 2021).

⁵⁴ Those will govern all transactions inside this world. Everything passes through the writing of a computer contract whose nature is unmodifiable and conditioned in time to the rules established in the contract itself, from buying and selling activities to commercial agreements, to private agreements. A smart contract can, indeed, regulate aspects of an economic nature and unlock certain features according to intermediate objectives that have been previously set.

⁵⁵ *Ibidem*.

⁵⁶ Art. 7, Italian Law no. 287/90.

⁵⁷ Art. 16, Italian Law no. 287/90; AGCM, Le operazioni di concentrazione: <https://www.agcm.it/competenze/tutela-della-concorrenza/operazioni-di-concentrazione/>.

provided that there are no conditions under which the merger falls within the competence of the EU Commission. M&A transactions in the digital market have been characterized by the payment of vast sums of money. For instance, WhatsApp, which at the time had only 32 engineers in its ranks, was bought by Facebook for \$22 billion⁵⁸. Considering 2015 and 2017, Alphabet (Google), Amazon, Apple, Facebook, and Microsoft completed 175 M&A transactions⁵⁹. These acquisitions fall under the category of “data-driven mergers”, i.e., transactions that aim to acquire, combine and/or monetize large amounts of valuable business data collected from multiple sources⁶⁰. These transactions often succeed in escaping merger control under competition law, and mainly concern acquisitions of potentially disruptive start-ups by super-dominant players.

In this regard, the European Commission recently published new Guidance on Article 22 of the Merger Regulation⁶¹. Indeed, DMA is characterized by an actual absence of any major proposed changes in merger control rules. Article 12 introduces an “obligation to inform about concentrations”. It is not merger control notification, but a way for the Commission to be informed in real-time. The reason is probably to be linked to the matter that the legal foundation for the DMA is the internal market (Art. 114 TFEU)⁶². In contrast, prohibitions against killer acquisitions would almost certainly have to be based on market dominance instead (Art. 102 TFEU). With the new Guidance on Article 22, even if there is no national jurisdiction in the first place, the Commission will accept referrals of concentrations from Member States. In other words, it is about mergers that take place below national thresholds and unreported either nationally or

⁵⁸ Ellie Zolfagharifard, “Facebook completes its \$22 billion acquisition of WhatsApp after European regulators give the green light”, *Daily Mail Online*, October 7, 2014, <https://www.dailymail.co.uk/sciencetech/article-2782370/Facebook-completes-19-billion-acquisition-WhatsApp-European-regulators-green-light.html>.

⁵⁹ Massimo Motta et al., “Big tech mergers”, *Information Economics and Policy* 54 (2021): 100868. <https://doi.org/10.1016/j.infoecopol.2020.100868>.

⁶⁰ Andressa Lin Fidelis, “Data-driven mergers: A call for further integration of dynamics effects into competition analysis”, *Revista de Defesa da Concorrência* 5, no. 2, 2020, 190.

⁶¹ European Commission, *Communication from the Commission: Commission Guidance on the application of the general mechanism set out in art. 22 of the Merger Regulation to certain categories of cases*, Brussels, (C(2021)1959), https://ec.europa.eu/competition/consultations/2021_merger_control/guidance_article_22_referrals.pdf.

⁶² Alfonso Lamadrid de Pablo et al., “Why the proposed DMA might be illegal under article 114 TFEU, and how to fix it”, *Journal of European Competition Law & Practice* 12, no. 7 (2021): 576-589, <https://doi.org/10.1093/jecclap/lpab059>.

at the EU level. However, such an approach is hardly enough. The major problem is understanding and predicting the future implication of M&A in a segment that might not yet exist or be relevant. Technologies and markets evolve rapidly, and antitrust authorities should analyse whether the acquired firm constitutes a potential competitor. Another outcome of the fast-paced evolving digital ecosystem is that market boundaries and barriers can change rapidly: complementary products might become substitutable.

Indeed, bringing back the attention to the virtual reality landscape – Facebook has already completed several acquisitions that could essentially be compared to the previously stated ones. It bought BigBox VR, Unit 2 Games, Beat Games, Sanzaru Games and Ready at Dawn. Besides, one day after becoming Meta, Facebook announced the acquisition of Within, a Los Angeles-based start-up behind the virtual-reality workout app Supernatural. Not forgetting the significant Oculus acquisition⁶³.

One may argue that Facebook is not the leader in virtual reality right now, but was it in social media networking?

FTC Commissioner Rebecca Slaughter stated “I think of serial acquisitions as a Pac-Man strategy. Each individual merger, viewed independently, may not seem to have significant impact. But the collective impact of hundreds of smaller acquisitions can lead to a monopolistic behemoth”⁶⁴. The risk of having new killer mergers or monopolization through M&A is not to be underestimated.

Recently, the UK’s Competition and Markets Authority attempted to block Meta’s acquisition of search engine Giphy. The latter, even if representing an increased attention to the matter, leads to vast doubts. What are the actual outcomes of differentiated intervention between Countries (see also what is happening in Germany⁶⁵) without a uniformed strategy?

⁶³ The acquisition has been paid \$ 2 billion dollars. The Bundeskartellamt is examining an abuse proceeding linkage between Oculus and the Facebook network. Press release 10.12.20: https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2020/10_12_2020_Facebook_Oculus.html. Furthermore, the same Bundeskartellamt also included the assessment of the new Section 19a GWB in its Facebook/Oculus proceeding. Press release 28.01.2021: https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2021/28_01_2021_Facebook_Oculus.html.

⁶⁴ Lauren Feiner, “FTC signals a focus on noncompetes and reporting loopholes after study of tech mergers”, *CNBC*, September 15, 2021, <https://www.cnn.com/2021/09/15/ftc-presents-findings-from-study-of-small-tech-mergers.html>.

⁶⁵ The Bundeskartellamt holds that Google is of paramount significance for competition across markets within the meaning of Section 19a(1) GWB. The company has an economic position of power which gives rise to a scope of action across markets that is insufficiently controlled by com-

What can such a differentiated and individualist approach to innovation and regulation bring?

3.4. Data exploitation

The rise of digital platforms has been underpinned by the collection and exploitation of data, mediated by the processing by algorithms, which constitutes and enhances its value⁶⁶. It is well known that the mechanism on which social network platforms are based is the sharing of personal data between users, platforms, and businesses. The Cambridge Analytica scandal and other elements involving Meta apps have highlighted how much of Facebook's business model revolves around direct access to Meta users' data⁶⁷. Besides, Apple allegedly uses privacy protection of its users to harm app providers relying on Apple's mobile platform (iOS)⁶⁸.

There is already enormous difficulty in regulating the use of data worldwide. Added to this, privacy law is not well developed in the digital platform sphere. The GDPR does not contain any platform-specific provisions, and it imposes its main set of obligations on so-called data controllers. Art. 25 GDPR is not directed to developers and producers of platforms, but to controllers⁶⁹. Many authors have discussed the lack of attention of the GDPR in relation to social network platforms⁷⁰ (the same goes for the ePrivacy directive).

petition. Holding more than 80 per cent of the market shares, Google has a dominant position on the market for general search services in Germany and is the main search advertising provider. In addition, Google is a powerful provider of a wide range of services in Germany and reaches a large number of users. With regard to the marketing of online advertising, Google also offers advertising services with a wide reach covering the entire value chain.

⁶⁶ Laura Ammannati, "I 'signori' nell'era dell'algoritmo", *Diritto Pubblico*, Fascicolo 2 (maggio-agosto 2021), 13.

⁶⁷ See: Matthew Rosenberg et al, "How Trump consultants exploited the Facebook data of millions", *The New York Times*, March 19, 2019, <http://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>.

⁶⁸ Baris Yüksel, "Competition authorities to investigate mobile application store dominance", *Kluwer Competition Law Blog*, October 18, 2019, <http://competitionlawblog.kluwercompetition-law.com/2019/10/15/competition-authorities-to-investigate-mobile-application-store-dominance/>.

⁶⁹ Joris van Hoboken, "Smartphone platforms as privacy regulators", *Computer Law & Security Review* 41 (2021): 105557, <https://doi.org/10.1016/j.clsr.2021.105557>.

⁷⁰ See *ibidem*; Lee Bygrave, "Data protection by design and by default: Deciphering the EU's legislative requirements", *Oslo Law Review* 4, no. 2 (2017), 43; European Data Protection Supervisor, "Preliminary Opinion on privacy by design (EDPS Opinion 5/2018)", paragraph 37.

Moreover, relevant uncertainty and lack of uniformity are also present in the USA⁷¹. The use of data by digital platforms was not discovered recently, and we still have problems regulating such a behaviour today. To the latter, it is not clear if consumers actually understand what happens with their data, or if they give their consent simply because they think there is no other choice.

Following a study⁷² on the topic 91% of adults think consumers have lost control over how companies collect and use personal information. If already today regulators and enforcers meet criticalities in finding the correct approach, the metaverse will probably become a data-privacy nightmare. If it is already possible for digital platforms to know a lot about us, in the metaverse, platforms and advertising agencies will probably track data concerning: a) in which environment an individual goes, b) how long the individual remains in a certain place, c) the physiological responses to the environment and the interaction with other users and products. Metaverse will need the collecting of vast quantities and types of personal information. Obtaining proper data protection compliance in the metaverse will likely remain a challenge for companies engaging with customers. Additionally, interfacing with consumers through reality devices will conceivably permit to gather significantly more data than today. Not considering the impact in the work environment. Research shows that a 5-minute VR session results in 5.4 million data points about individual body language⁷³. It has been demonstrated that, out of a pool of 511 participants, the VR system identifies 95% of users correctly when trained on less than 5 min of tracking data per person⁷⁴. These results show that the public and researchers should understand nonverbal data as personally identifying data⁷⁵. The latter could lead the undertaking(-s) having the control on the metaverse to know the consumers in a way that today is not conceivable.

⁷¹ Unless a State has its own data privacy law, there are no updated federal privacy laws regulating this sector. See the State laws related to digital privacy on the National Conference of State Legislatures' website: <https://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx>.

⁷² Lee Rainie, "Americans' complicated feelings about social media in an era of privacy concerns", *Pew Research Center*, August 17, 2020, <https://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns>.

⁷³ Jeremy Dalton, *Reality Check: How Immersive Technologies Can Transform Your Business*. UK: Kogan Page, 106.

⁷⁴ Mark Roman Miller et al., "Personal identifiability of user tracking data during observation of 360-degree VR video", *Sci Rep* 10, 17404, <https://doi.org/10.1038/s41598-020-74486-y>.

⁷⁵ *Ibidem*.

For instance, being able to unconsciously lead a consumer who is walking into the parallel world to enter the meta-Nike store.

Heller and Bar-Zeev have warned that “when you think about advertising in XR, you should think about it as placement in the product instead of product placement”⁷⁶. If the provider that controls the dominant search engine (e.g., Google) and its dataset can disrupt neighbouring markets, imagine what will happen in the metaverse. The unstoppable pervasiveness of data and of the mechanisms that analyse and process them, such as algorithms, confront us with the fact that the ways of acquiring and managing data, as well as their nature and quality, is a crucial issue⁷⁷. For instance, the ability of these same players to organize and exploit data in real time and for purposes other than those of the activity that generated it (commercial use for marketing, profiling of consumers, advertising, etc.). Thus, blurring the lines between markets, changing how they are accessed, thwarting the legal rules of the organization, and amplifying the phenomenon of digital de-regulation. The platform’s power is largely dictated by the need to circumvent regulatory constraints⁷⁸.

This simple observation confronts us with the fact that data are an essential asset, an indispensable resource for the various economic activities or services that require their use to function, and whose value changes according to the applications or services for which the data are collected or required. Already as of today, online platforms possess a considerable amount of data that allows the prediction of consumers’ preferences⁷⁹. Thus, algorithms could be used as a never-ending cycle of extracting data, creating a nearly perfect marketing system controlled by AI that influences consumer choice⁸⁰. Besides, the dataset owned by the online platform will always increase its value, making it impossible for another market player to reach the same level. Such a dataset could effectively become a barrier precluding access to the market.

⁷⁶ Brittan Heller et al., “The problems with immersive advertising: In Ar/VR, nobody knows you are an ad”, *Journal of Online Trust and Safety* 1, no. 1 (2021), <https://doi.org/10.54501/jots.v1i1.21>.

⁷⁷ *Ibidem*.

⁷⁸ *Ibidem*.

⁷⁹ Centre for Data Ethics and Innovation, *Review of online targeting: Final report and recommendation* (February 2020) (CDEI report), 14.

⁸⁰ Enrique Bravo-Garcia et al., “Introducing nudging algorithms”, *Kluwer Competition Law Blog*, July 23, 2020, http://competitionlawblog.kluwercompetitionlaw.com/2020/07/23/introducing-nudging-algorithms/#_ftn19.

Circling back to centralization, the CMA already expressed in 2020 as, alongside Facebook, Google has “a clear incentive to apply a stricter interpretation of the requirements of data protection regulation when it comes to sharing data with third parties than for the use and sharing of data within [its] own ecosystem”⁸¹.

Furthermore, as an example of a nudging algorithm, the European Commission fined Google €2.42M for leveraging its market power on general search engines into price comparison websites⁸². The algorithm nudges consumers into using another service provided by Google⁸³. If the provider that controls the dominant search engine (i.e., Google) and its dataset can disrupt neighbouring markets, imagine what will happen in the metaverse.

How will another new-entry player be able to reach such a data set on which the metaverse profits will be based? Moreover, the most crucial among the vast potentially arising questions is: how will authorities be able to control the environment and enforce competitors and citizens’ rights?

4. Should regulation play a role?

There are relevant criticalities for competition public enforcement in the development of the metaverse – not considering the impact on other subjects, such as privacy, IP, financial markets.

The question is whether to intervene or wait for the market to develop (and only then think about what to do). To start, it might be relevant to examine the effects of the so-called pacing problem. Regulatory reforms must consider the link between regulation and innovation. Indeed, innovation impacts regulation and, equally, regulation can affect the innovation process⁸⁴. Regulatory interventions are normally a response to economic and social conditions; thus, also by technological developments affecting the general environment⁸⁵. Indeed, in all areas, regulatory intervention should have the result to yield benefits as far as decreasing expenses, improving efficiency and stimulating development.

⁸¹ CMA, “Online platforms and digital advertising”, *Market study final report*: <https://assets.publishing.service.gov.uk/media/5efc57ed3a6f4023d242ed56/Finalreport1July2020.pdf>.

⁸² Google Search (Shopping) Case AT.39740, https://ec.europa.eu/competition/antitrust/cases/dec_docs/39740/39740_14996_3.pdf.

⁸³ Enrique Bravo-Garcia et al., “Introducing nudging algorithms”, 20.

⁸⁴ Knut Blind et al., “The impact of standards and regulation on innovation in uncertain markets”, *Research Policy* 46, no. 1 (2017), <https://doi.org/10.1016/j.respol.2016.11.003>.

⁸⁵ OECD, *Regulatory Reform and Innovation*, <https://www.oecd.org/sti/inno/2102514.pdf>.

Regulatory shifts could be controversial in rearranging the expenses of public policies among economic actors and adjusting set up frameworks of insurance, regardless of whether for industry or consumers. Some authors argue that strict policies slow the rate of technology developments⁸⁶. Others, that regulation favours it, and that its absence could actually have the opposite effects⁸⁷. In order to achieve a functional relation between competition regulation and innovation, it is essential to 1) properly understand the new technology and have an oversight on potential effects; 2) balance the relation between competition and innovation; 3) avoid regulations that can represent a burden to the pace requested by innovation; and 4) be harmonized internationally, to avoid conflicting regulation and barriers⁸⁸.

Just as technology needs a particular regulatory approach to foster its development, in the same way, disruptive technologies arrive more frequently and at a faster pace than the decision on whether and how to intervene. Adapting the regulatory framework to address increasing and growing concerns related to disruptive technologies turned out to be progressively crucial. Clearly, it is not an easy task to design a framework able to ensure the safety of users, respect for their rights and facilitate innovation. Even more, considering that this is an environment at a fast pace, and traditional regulation might not be suitable.

The Big Techs are not famous for their availability to regulatory compliance. Examples of inadequate self-regulation and oversights are easy to find: Facebook's mis/disinformation and recent scandal on its algorithm is the latest⁸⁹. Other Big Techs' relation with competition and data protection authorities (and fines or not respected obligations) is almost daily news. For instance, hearings by the House Antitrust Subcommittee have revealed substantial evidence of how Big Tech has sustained and expanded their market dominance with anticompetitive practices⁹⁰.

⁸⁶ Carl A. Futia, "Schumpeterian competition", *The Quarterly Journal of Economics* 94, no. 4 (1980), 675, <https://doi.org/10.2307/1885663>.

⁸⁷ Kenneth J. Arrow et al., "Existence of an equilibrium for a competitive economy" *Econometrica* 22, no. 3 (1953), 265-290, <https://doi.org/10.2307/1907353>.

⁸⁸ OECD, *Regulatory Reform and Innovation*, <https://www.oecd.org/sti/inno/2102514.pdf>.

⁸⁹ Keach Hagey et al., "Facebook tried to make its platform a healthier place. It got angrier instead", 24.

⁹⁰ Tim Wheeler, "Tech and antitrust: Pay attention to the math behind the curtain", *Brookings.edu*, <https://www.brookings.edu/blog/techtank/2020/07/31/big-tech-and-antitrust-pay-attention-to-the-math-behind-the-curtain/>.

Moreover, it has been stated that delayed regulation does not allow power to do much against platforms, resulting in systemic compliance issues and risk to democracy and market stability⁹¹. A fact-based approach to regulation could have worked with less fast innovation cycles and innovations developed in decades. Thus, having the possibility to prior understand the risks and balance risk assessment, intended as scientific analysis, with risk management, intended as policy intervention.

The lack of prior understanding of the technology and the delayed regulation led to undertakings that became essential infrastructure for society, continuing to grow with the strongest possible lobbying power. At the same time, regulators start to understand how to intervene⁹². There might still be time to intervene to avoid what happened with technologies that already changed our everyday life, and the metaverse might have even deepest effects on the market. This is to circumvent, for instance, selling consumers' data without consent, ensuring users' control and companies' support. Bear in mind that the metaverse will be based on blockchain technology and the latter uses ledgers to which data can be added. However, by design, blockchain is not meant for removing data from the chain⁹³.

It then appears clear that regulatory intervention for competition public enforcement is already needed in a first-phase development of the metaverse. In light of the above-described characteristics of the metaverse, of the related criticalities – and of the need for regulatory intervention – possible remedies to address the potential issues must be hypothesized.

It becomes relevant to understand which approach might be appropriate. Indeed, the OECD highlights five questions regulators need to ask themselves: 1) what is the current state of regulation?; 2) what is the right time to regulate?; 3) is regulation the right approach?; 4) what is the right regulatory approach? and 5) what has changed since regulations were enacted?⁹⁴. To the first three questions, when possible, an answer has been given above. The last question cannot be answered at this stage. The focus shall then go on the fourth one. Regulation does not come in a one type formula and as such can have multiple effects based on how it is structured. Obviously,

⁹¹ *Ibidem*.

⁹² "Archives". *Harvard Gazette*, June 26, 2019, <https://news.harvard.edu/gazette/page/96/?p=mycmkwhixz.html>.

⁹³ Martin Florian et al., "Erasing data from blockchain nodes", *2019 IEEE European Symposium on Security and Privacy Workshops (EuroSec&PW)*, 2019, <https://doi.org/10.1109/eurospw.2019.00047>.

⁹⁴ OECD, "Regulatory policy in the Slovak Republic: Towards future-proof regulation", *OECD Reviews of Regulatory Reform*, OECD Publishing, Paris, <https://doi.org/10.1787/ce95a880-en>.

the impact of regulation on technology critically depends on the chosen type of regulation. Different regulatory approaches can impede or accelerate technological developments or shape them differently, favouring some technologies, or firms, instead of others. *Ex post* regulation is considered to be a) backward looking, b) adopting a narrow view of products markets driven primarily by demand-side substitutability, c) focused on strategic behaviour suited to retail level abuses, d) fact specific, e) resulting in declaratory remedies in nature and best enforced through civil courts. On the opposite, *ex ante* regulation is considered to be a) forward looking, 2) likely to identify or to define markets in broader terms based as much on the forces of supply as those of demand, c) focused on addressing market failures driven by the logic of a certain industry structure, d) specific and detailed in the prescription of remedies and in terms of parameters⁹⁵. The examples of ‘recent’ regulatory interventions, from internet to artificial intelligence, shows that – when considering emerging technologies with fast-paced development – failing to take early steps to structurally regulate a given sector or entity leads to “controlling regulation” and “risk managing” in the hands of the big market players⁹⁶. The above leads to excluding *ex post* regulation. Indeed, the effectiveness and speed of enforcement to tackle Big Techs’ behaviour, and the consequences of delayed regulation, led towards preferring an *ex-ante* regulatory framework⁹⁷. *Ex post* remedies risk being slow in time response and ineffective to protect consumers and market competition. An *ex-ante* regulatory decision is based on the analysis of the risk posed by the product or service or sector development. This requires a balance between various factors. Firstly, a balance between science-based risk assessment and risk management by policy makers, with the addition of risk communication handling between competent authorities. On a second base, a balance between risk perception by the public and the scientific world, and the communication of the risk and adequacy of intervention to the public. An *ex-ante* approach based on risk requires identifying and managing the risk in a fast process⁹⁸. This is an

⁹⁵ *Ibidem*.

⁹⁶ Julia Black and Andrew Murray, “AI and machine learning: Setting the regulatory agenda”, *European Journal of Law and Technology* 10, no. 3 (2019), 23.

⁹⁷ “Big tech regulation: What is going on?”, *Bis.org*, <https://www.bis.org/fsi/publ/insights36.pdf>.

⁹⁸ As widely known, this is also linked to the precautionary principle, for such situations in which evidence is not sufficient and hard to be proven at that stage. However, with reasonable ground for concerns to the public or the environment, so that the burden of proof is on the producer of the risk to prove the lack of harmfulness.

approach that has been strongly referred to as being the correct one for artificial intelligence, so to foster it while protecting markets and consumers. However, risk involves a causal relationship between the event and the not-to-be desired outcome. Indeed, it is necessary to quantify the probabilities of the event and the cost/benefit analysis of an accident. It is a different situation when uncertainty is the topic to deal with⁹⁹.

In the metaverse, at least at the beginning, “risk” will be difficult to identify and not instantly evident; while entering a parallel virtual world, uncertainty will be the describing word. Thus, an *ex-ante* regulatory risk-based approach is surely needed but not enough on its own. Current theories of regulation, if singularly used, are poorly equipped to face emerging technologies. Uncertainty leads to regulators not being able to understand what approach to use and thus intervene. To regulate uncertainty, the regulatory approach should be characterized by strategic foresight¹⁰⁰. The latter is the discipline that explores a range of plausible alternative futures and their implications. It has recently been defined in the EU Better Regulation toolbox as the discipline of exploring, anticipating, and shaping the future into policymaking¹⁰¹. This by assuring a future-oriented analysis of the problem drivers (so-called megatrends) and the future scenarios. Among the megatrends of the EU 2021 strategic foresight report¹⁰² are digital hyperconnectivity and digital transformation.

To these general ones, others easily applicable to the metaverse are: virtual connectivity, extremely personalized environment, risk of fragmentation and separation of network and services, digital divide/inclusion, data quantity and quality growth and more sophisticated networks, that consent a more efficient use of artificial intelligence predictive systems.

As per the toolbox, having identified the potential megatrends, attention should now be oriented towards a regulatory future-proof intervention. Uncertainty is not taken in enough consideration, even if it heavily

⁹⁹ Kyeonggook Francis Park et al., “Risk and uncertainty”, in Mie Auger et al. (eds). *The Palgrave Encyclopedia of Strategic Management*. Palgrave Macmillan, London. https://doi.org/10.1057/978-1-349-94848-2_250-1.

¹⁰⁰ Tamra Lysaght, “Anticipatory governance and foresight in regulating for uncertainty”, *The American Journal of Bioethics* 22, no. 1 (2021), 51-53, <https://doi.org/10.1080/15265161.2021.2001111>.

¹⁰¹ European Commission, “Better regulation toolbox 2021”, 155.

¹⁰² European Commission, “Communication from the Commission to the European Parliament and the Council. 2021 Strategic Foresight Report. The EU’s capacity and freedom to act” (2021/COM/2021/750 final), 10.

affects regulatory intervention development, and the same competent institutions. To tackle uncertainty and assure future-proof intervention efficiency, it is not sufficient to use one approach or tool. What is crucial is allowing systematic and gradual application of different approaches to reach a foresight governance¹⁰³. Following Milliken, uncertainty might be: 1) state uncertainty, which relates to the inability to predict future scientific discoveries and the launch of applications of the new technology; 2) effect uncertainty associated with the inability to predict the impact of the emerging technology on particular stakeholders' organizations; and 3) response uncertainty, linked to the inability to predict which regulatory tools are more suitable to the specific features of the emerging technology¹⁰⁴. These types of uncertainty are at the centre of the immobilization of the regulatory development process.

An essential step would be laying institutional foundations for the establishment of an international regulatory co-operation and joined up-approaches. The latter to provide a borderless framework of the meta-verse regulation, since the metaverse itself will be a virtual world without borders. Besides, it should be added (to the overall approach) the idea of adapting the governance frameworks to enable the development of agile and future-proof regulation¹⁰⁵. Therefore, to avoid an essential facility excluding competitors by design, regulators must first of all be included in the development of the infrastructure. Before that, the first requirement of the essential facility doctrine should be reviewed in the definition of "a new product, which the dominant firm did not offer". An already existing product/service must be included, but with different characteristics that can equally attract a strong consumer demand. In a strong oversight on the metaverse development (due to metaverse potentially being more than a service, close to a new market segment), regulators and enforcers should have a continuous and open discussion with the infrastructure provider, other market participants, and technical experts. The latter to assure that the infrastructure is structured in a way that, from the beginning, easily allows the use of third-party internal and external tools. Thus, granting

¹⁰³ OECD, *Regulatory Policy in the Slovak Republic: Towards Future-Proof Regulation* (OECD Reviews of Regulatory Reform, OECD Publishing, Paris, 2020), 20.

¹⁰⁴ Discussed in Frances J. Milliken, "Three types of perceived uncertainty about the environment: state, effect, and response uncertainty", *The Academy of Management Review* 12, no. 1 (1987), 133-143.

¹⁰⁵ See OECD, "Recommendation of the Council for agile regulatory governance to harness innovation", 2021, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0464>, 30.

access rights. For instance, by using code parameters that allow the same compatibility and potential use of all the musical services, as Spotify, Apple music, etc.

The central role of an oversight of regulators on the metaverse would lie in assuring the development of a facility open to competitors' access. This would also be an opportunity for the undertaking involved to be *ex-ante* sure of respecting the rules. To this aim, it could be useful to establish internal assessment mechanisms for auto-detecting issues in the metaverse source code. This could be seen as a form of co-regulation.

Concerning collusion, three interventions should be considered. The first one is the widely discussed sandbox testing. In particular, including a shadow environment inside the metaverse. Thus, a minor reproduction of the metaverse for beta-testing, in which authorities and interested parties can evaluate the functioning and behaviour of the algorithm, before the implementation in the real metaverse (a proper risk assessment phase). However, the regulatory framework should also evolve considering the undertakings that profit from the tacit collusion liable, even if no proof of an agreement is to be found. Indeed, an antitrust authority cannot sanction tacit collusion in case of intelligent adaptation by the firms¹⁰⁶. The tested algorithm should also be built in a way that its evaluations may be monitored (e.g., by data mining). Besides, authorities' algorithm could be included, designed to alert price changes that need to be investigated. Another main tool that might be used, to prevent both algorithmic and blockchain collusion, is market surveillance. Indeed, algorithmic market surveillance would allow to identify alleged anti-competitive price setting behaviour, and then have the power to implement inspections to verify the colluding behaviour (for instance, also through the possibility of remotely accessing the servers/devices of the undertakings). The use of regulatory experiments will allow to test the future implications and set the regulation on stakeholders' feedback.

On M&A, the approach should be uniformed between Countries. Indeed, even EU Member States are leaning towards different approaches to the matter (see *Germany v UK*, in p. 17). Having different regulations and tools leads to a lack of certainty, which impacts adversely both undertakings and enforcers. Then, the main concern for authorities is to evaluate

¹⁰⁶ See European Commission, "Algorithms and collusion – Note from the European Union", 2017, [https://one.oecd.org/document/DAF/COMP/WD\(2017\)12/en/pdf](https://one.oecd.org/document/DAF/COMP/WD(2017)12/en/pdf).

M&A for which a market segment does not yet exist or is considered to be relevant. Authorities' involvement in the development of the metaverse will give them the ability to previously understand what types of services and specific segments are observed by undertakings. Therefore, the key elements here would be international regulatory co-operation and management-based regulation.

On data exploitation, the elements to take into account are various. First of all, the consumer point of view. Consumers tend to have an adversity on losing control in face of uncertainty, unless they are dealing with trusted business partners or individuals¹⁰⁷. The relation between consumers and one of the Big Techs would hardly be characterized by trust. Moreover, the combination between the loss aversion and *status quo* biases represents as, unless there is a very profitable input to change, individuals prefer to stay on the safe side¹⁰⁸. Indeed, it is generally given more value to the loss than the gain¹⁰⁹. However, giving value to the loss of data requires a high level of awareness from the consumer, being a loss that does not directly bring a negative feeling compared to the digital environment gains. In case of actual presence of the elements of desired control and loss aversion, a control model might help both consumers' certainty and data exploitation. A potential tool would be a personal tracker, based on the idea of cookies. Whoever wants to keep track of the use of his data, may insert this tracker (e.g., through a plug-in or a specific device) and follow how the information is spread on the metaverse. Besides, to solve the market power given by the amount of data stored by major undertakings¹¹⁰, the small undertakings could ask the major undertaking for the dataset. Automatically, the consumer would receive an alert and decide whether to consent to the transfer of the data between firms, knowing exactly who is asking and why. This would also limit the data transactions market without users' informed consent.

¹⁰⁷ Bing-Sheng Teng et al., "Between trust and control: Developing confidence in partner cooperation in alliances", *Academy of Management Review* 23, no. 3 (1998), 491-512, <https://doi.org/10.5465/amr.1998.926623>.

¹⁰⁸ Sendhil Mullainathan and Richard H. Thaler, "Behavioral economics", *International Encyclopedia of the Social & Behavioral Sciences*, 2015, 437-442, <https://doi.org/10.1016/b978-0-08-097086-8.71007-5>.

¹⁰⁹ *Ibidem*.

¹¹⁰ See Marco Gambaro, "Big Data competition and market power", *Market and Competition Law Review* II, no. 2 (2018), 99-122.

Lastly, also concerning commitments, the smart contract tool could be used in the relationship between authorities and undertakings. If a firm commits not to raise or reduce prices more than a given percentage, the smart contract will monitor such a behaviour and proceed with the established consequence if this is not respected.

5. Conclusions

In light of the above, the first result is that the over-discussed decentralized future of the metaverse will never exist as conceptualized. Even if some tools (i.e., blockchain) might be decentralized, this will probably not be reflected in the infrastructure that will host the metaverse. Its users will not control the latter. It will be controlled, but by the same – or also new – few leading characters.

The paper tries to show as such a structured virtual world might bring several antitrust concerns, starting from the potential essential facilities doctrine applicability, tacit collusion, old M&A concerns, and the historically unsolved data exploitation issue.

A regulatory intervention is needed. The latter will have to be characterized by a strategic foresight approach, which includes anticipatory regulation and the concurrent or gradual application of various regulatory approaches, based on the specific situation. A regulatory cooperation in building the metaverse is the key. Having regulators inside the development process and establishing a proactive dialogue between the two, with undertakings knowing that authorities will predict and continuously monitor antitrust practices.

To allow a foresight approach, agile and adaptive regulation is crucial. One should not only avoid having rules that suppress innovation, but also norms that suppress the applicability of adaptive regulatory approaches.

Bibliography

- “Definitions, meanings, & Spanish translations”. *Lexico Dictionaries | English*. <https://www.lexico.com/>.
- “Founder’s letter, 2021”. Meta. October 29, 2021. <https://about.fb.com/news/2021/10/founders-letter/>.
- “Open-source P2P money”. *Bitcoin*. <https://bitcoin.org/bitcoin.pdf>.
- “The Facebook Company is now Meta”. *Meta*. November 23, 2021. <https://about.fb.com/news/2021/10/facebook-company-is-now-meta/>.

- “The impact of blockchain technology on finance: A catalyst for ... – voxeu”. <https://voxeu.org/system/files/epublication/Geneva21.pdf>.
- “The Metaverse: The evolution of a universal digital platform”. *Global law firm | Norton Rose Fulbright*. <https://www.nortonrosefulbright.com/en/knowledge/publications/5cd471a1/the-metaverse-the-evolution-of-a-universal-digital-platform>.
- “Watch Mark Zuckerberg play Jenga and Fist-Bump in virtual reality using ‘haptic gloves’ that Facebook, now Meta, is building to let people feel objects in the Metaverse”. *Yahoo! News*. <https://news.yahoo.com/watch-mark-zuckerberg-play-jenga-234930754.html>.
- Ammannati, Laura. “I ‘signori’ nell’era dell’algoritmo”. *Diritto Pubblico*, no. 2 (2021): 13.
- Arrow, Kenneth J., and Gerard Debreu. “Existence of an equilibrium for a competitive economy”. *Econometrica* 22, no. 3 (1954): 265. <https://doi.org/10.2307/1907353>.
- Bailenson, Jeremy. “Protecting nonverbal data tracked in virtual reality”. *JAMA Pediatrics* 172, no. 10 (2018): 905. <https://doi.org/10.1001/jamapediatrics.2018.1909>.
- Black, Julia, and Andrew Murray. “AI and machine learning: Setting the regulatory agenda”. *European Journal of Law and Technology* 10, no. 3 (n.d.).
- Blind, Knut, Sören S. Petersen, and Cesare A.F. Riillo. “The impact of standards and regulation on innovation in uncertain markets”. *Research Policy* 46, no. 1 (2017): 249-264. <https://doi.org/10.1016/j.respol.2016.11.003>.
- Bodó, Balázs, Jaya Klara Brekke, and Jaap-Henk Hoepman. “Decentralisation: A multidisciplinary perspective”. *Internet Policy Review* 10, no. 2 (2021). <https://doi.org/10.14763/2021.2.1563>.
- Brekke, Jaya Klara. “Hacker-engineers and their economies: The political economy of decentralised networks and ‘cryptoeconomics’”. *New Political Economy* 26, no. 4 (2020): 646-659. <https://doi.org/10.1080/13563467.2020.1806223>.
- Bygrave, Lee A. “Data protection by design and by default: Deciphering the EU’s legislative requirements”. *Oslo Law Review* 4, no. 2 (2017): 105-120. <https://doi.org/10.18261/issn.2387-3299-2017-02-03>.
- Cohen, Julie E. “Between Truth and Power,” 2019. <https://doi.org/10.1093/oso/9780190246693.001.0001>.
- Commission, European, ed. “Communication from the Commission to the European Parliament and the Council. 2021 Strategic Foresight Report. The EU’s Capacity and Freedom to Act (2021/COM/2021/750 Final).,” n.d.
- Coulter, Martin. “Mark Zuckerberg and Sundar Pichai personally oversaw an illegal deal that misled publishers and advertisers, unredacted suit alleges”. *Business Insider*. January 17, 2022. <https://www.businessinsider.com/google-and-facebook-execs-allegedly-signed-off-illegal-ads-deal-2022-1?r=US&IR=T>.

- D'Alberti, Marco. "Concorrenza e giustizia sociale". *Mercato Concorrenza Regole*, no. 2 (2020): 14.
- Das, T. K., and Bing-Sheng Teng. "Between trust and control: Developing confidence in partner cooperation in alliances". *Academy of Management Review* 23, no. 3 (1998): 491-512. <https://doi.org/10.5465/amr.1998.926623>.
- Davis, Alanah, John Murphy, Dawn Owens, Deepak Khazanchi, and Ilze Zigurs. "Avatars, people, and virtual worlds: Foundations for research in Metaverses". *Journal of the Association for Information Systems* 10, no. 2 (2009): 90-117. <https://doi.org/10.17705/1jais.00183>.
- European Commission, Communication from the Commission to the European Parliament and the Council. 2021 Strategic Foresight Report. The EU's capacity and freedom to act (2021/COM/2021/750 final).
- European Commission. "2021 merger control". *Competition Policy*. https://ec.europa.eu/competition-policy/public-consultations/2021-merger-control_en.
- European Commission. "Better regulation toolbox". December 7, 2021. https://ec.europa.eu/info/law/law-making-process/planning-and-proposing-law/better-regulation-why-and-how/better-regulation-guidelines-and-toolbox/better-regulation-toolbox-0_en.
- Ezrachi, Ariel, and Maurice E. Stucke. "Sustainable and unchallenged algorithmic tacit collusion". *SSRN Electronic Journal*, 2018. <https://doi.org/10.2139/ssrn.3282235>.
- Florian, Martin, Sebastian Henningsen, Sophie Beaucamp, and Bjorn Scheuermann. "Erasing data from blockchain nodes". *2019 IEEE European Symposium on Security and Privacy Workshops (EuroSec&PW)*, 2019. <https://doi.org/10.1109/eurospw.2019.00047>.
- Futia, Carl A. "Schumpeterian competition". *The Quarterly Journal of Economics* 94, no. 4 (1980): 675. <https://doi.org/10.2307/1885663>.
- Gambaro, Marco. "Big Data competition and market power". *Market and Competition Law Review* 2, no. 2 (2019): 99-122. <https://doi.org/10.7559/mclawreview.2018.326>.
- Gong, Xiaowen, Lingjie Duan, Xu Chen, and Junshan Zhang. "When social network effect meets congestion effect in wireless networks: Data usage equilibrium and optimal pricing". *IEEE Journal on Selected Areas in Communications* 35, no. 2 (2017): 449-462. <https://doi.org/10.1109/jsac.2017.2659059>.
- Hagey, Keach, and Jeff Horwitz. "Facebook tried to make its platform a healthier place. It got angrier instead". *The Wall Street Journal*. September 15, 2021. <https://www.wsj.com/articles/facebook-algorithm-change-zuckerberg-11631654215>.
- Halsmayer, Verena.[Recension: "Philip Mirowski, Edward Nik-Khah, *The Knowledge We Have Lost in Information: The History of Information in Modern Economics*. Oxford: Oxford University Press 2017". *Berichte zur Wissenschaftsgeschichte* 41, no. 4 (2018): 484-485. <https://doi.org/10.1002/bewi.201801943>.

- Heller, Brittan, and Avi Bar-Zeev. "The problems with immersive advertising: In AR/VR, nobody knows you are an ad". *Journal of Online Trust and Safety* 1, no. 1 (2021). <https://doi.org/10.54501/jots.v1i1.21>.
- Kamin, Debra. "Investors snap up Metaverse real estate in a virtual land boom". *The New York Times*. November 30, 2021. <https://www.nytimes.com/2021/11/30/business/metaverse-real-estate.html>.
- Lamadrid de Pablo, Alfonso, and Nieves Bayón Fernández. "Why the proposed DMA might be illegal under article 114 TFEU, and how to fix it". *Journal of European Competition Law & Practice* 12, no. 7 (2021): 576-589. <https://doi.org/10.1093/jeclap/lpab059>.
- lauren_feiner. "FTC signals a focus on noncompetes and reporting loopholes after study of tech mergers". *CNBC*. September 15, 2021. <https://www.cnbc.com/2021/09/15/ftc-presents-findings-from-study-of-small-tech-mergers.html>.
- Lin Fidelis, Andressa. "Data-driven mergers: A call for further integration of dynamics effects into competition analysis". *Revista de Defesa da Concorrência* 5, no. 2 (2020).
- Lysaght, Tamra. "Anticipatory governance and foresight in regulating for uncertainty". *The American Journal of Bioethics* 22, no. 1 (2021): 51-53. <https://doi.org/10.1080/15265161.2021.2001111>.
- Martín-Laborda, Antonio Robles. "Merger Control and Online Platforms: The Relevance of Network Effects". *Market and Competition Law Review* 1, no. 2 (2017): 69-100. <https://doi.org/10.7559/mclawreview.2017.350>.
- McKenzie, Richard, and Dwight Lee. "In defense of monopoly," 2008. <https://doi.org/10.3998/mpub.93419>.
- Miller, Mark Roman, Fernanda Herrera, Hanseul Jun, James A. Landay, and Jeremy N. Bailenson. "Personal identifiability of user tracking data during observation of 360-degree VR video". *Scientific Reports* 10, no. 1 (2020). <https://doi.org/10.1038/s41598-020-74486-y>.
- Milliken, Frances J. "Three types of perceived uncertainty about the environment: State, effect, and response uncertainty". *Academy of Management Review* 12, no. 1 (1987): 133-143. <https://doi.org/10.5465/amr.1987.4306502>.
- Motta, Massimo, and Martin Peitz. "Big tech mergers". *Information Economics and Policy* 54 (2021): 100868. <https://doi.org/10.1016/j.infoecopol.2020.100868>.
- Mullainathan, Sendhil, and Richard H. Thaler. "Behavioral economics". *International Encyclopedia of the Social & Behavioral Sciences*, 2015, 437-442. <https://doi.org/10.1016/b978-0-08-097086-8.71007-5>.
- Nicolaidis, Phedon. "A theory of regulatory integration". *Intereconomics* 41, no. 1 (2006): 37-43. <https://doi.org/10.1007/s10272-006-0170-y>.

- OECD. “Algorithms and collusion: Competition policy in the digital age”. <https://www.oecd.org/competition/algorithms-collusion-competition-policy-in-the-digital-age.htm>.
- OECD. “Regulatory policy in the Slovak Republic: Towards future-proof regulation (OECD reviews of regulatory reform”. OECD Publishing, Paris, 2020.
- OECD. “Regulatory reform and innovation”. <https://www.oecd.org/sti/inno/2102514.pdf>.
- Park, K. Francis, and Zur Shapira. “Risk and uncertainty”. *The Palgrave Encyclopedia of Strategic Management*, 2017, 1-7. https://doi.org/10.1057/978-1-349-94848-2_250-1.
- Patton, Michael Quinn. “Process use as a usefulness”. *New Directions for Evaluation* 2007, no. 116 (2007): 99-112. <https://doi.org/10.1002/ev.246>.
- Rosenberg, Matthew, Nicholas Confessore, and Carole Cadwalladr. “How Trump consultants exploited the Facebook data of millions”. *The New York Times*. March 17, 2018. <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>.
- Schneider, Nathan. “Decentralization: An incomplete ambition”. *Journal of Cultural Economy* 12, no. 4 (2019): 265-285. <https://doi.org/10.1080/17530350.2019.1589553>.
- Schrepeel, Thibault. “Collusion by blockchain and smart contracts”. *SSRN Electronic Journal*, 2019. <https://doi.org/10.2139/ssrn.3315182>.
- Schrepeel, Thibault. “The fundamental unimportance of algorithmic collusion for anti-trust law”. <https://jolt.law.harvard.edu/digest/the-fundamental-unimportance-of-algorithmic-collusion-for-antitrust-law>, n.d.
- Schrepeel, Thibault. *Blockchain + Antitrust: The Decentralization Formula*. Cheltenham, UK: Edward Elgar Publishing Limited, 2021.
- Stephenson, Neal. *Snow Crash*. Milano: Rizzoli, 2007.
- Stolton, Samuel. “Vestager: Metaverse poses new competition challenges”. *POLITICO*. January 19, 2022. <https://www.politico.eu/article/metaverse-new-competition-challenges-margrethe-vestager/>.
- Strong, A., and S. Baker. “How will autonomous vehicle technologies affect driver liability and overall insurance?” *Autonomous Passenger Vehicles*, 2015. <https://doi.org/10.1049/ic.2015.0064>.
- van Hoboken, Joris, and R Ó Fathaigh. “Smartphone platforms as privacy regulators”. *Computer Law & Security Review* 41 (2021): 105557. <https://doi.org/10.1016/j.clsr.2021.105557>.
- Westland, J. Christopher. “Critical mass and willingness to pay for social networks”. *Electronic Commerce Research and Applications* 9, no. 1 (2010): 6-19. <https://doi.org/10.1016/j.eierap.2009.05.003>.

Zolfagharifard, Ellie. "Facebook completes its \$22 billion acquisition of WhatsApp after European regulators give the green light". *Daily Mail Online*. October 7, 2014. <https://www.dailymail.co.uk/sciencetech/article-2782370/Facebook-completes-19-billion-acquisition-WhatsApp-European-regulators-green-light.html>.

Zwitter, Andrej, and Jilles Hazenberg. "Decentralized network governance: Blockchain technology and the future of regulation". *Frontiers in Blockchain* 3 (2020). <https://doi.org/10.3389/fbloc.2020.00012>.