Platforms in the Age of Metaverse: Sustainability by Proportionality

Giovanni De Gregorio[*], Pietro Dunn[•] and Oreste Pollicino[°]

Abstract

The metaverse represents the new frontier of the digital space and will likely bring new challenges as well as unprecedented opportunities like other digital environments. The time is ripe, therefore, to initiate a debate on the paradigm brought by the metaverse, with a view to ensure, on the one hand, the protection of fundamental rights and freedoms, as well as of democratic values, and, on the other hand, avoid the strangling of technological development and innovation. In other words, the primary challenge is to strike a balance between the rush towards innovation and the overprotection and enforcement of rights that could lead to disproportionate measures, thus making the building of the metaverse an economically unsustainable effort for platforms. Focusing on privacy and content moderation and adopting a European constitutional perspective, the present work highlights the importance of guaranteeing that the law and its enforcement primarily focus on the principle of proportionality that is then translated by the risk-based approach of EU digital policies. As the primary lodestar of European constitutionalism, proportionality will thus be essential to promote a sustainable evolution of the metaverse that looks at the various interests at stake, including economic freedoms, to correctly balance and respect them at their core.

1. Introduction

The metaverse is expanding and promises to provide new opportunities to offer products and services, thus making digital technologies increasingly part of daily life. Many fields and areas are increasingly influenced by the metaverse, which may come to play an increasingly central role, and the many improvements that this space promises to achieve.[1] Nonetheless, even if the metaverse is likely to bring new opportunities, it also raises questions for the protection of rights and freedoms that reverberate, in turn, on the question concerning the sustainability of platform

[*] PLMJ Chair in Law and Technology, Católica Global School of Law, Lisbon.
[•] PhD Candidate in Law, Science and Technology, University of Bologna.
[°] Full Professor of Constitutional Law, Bocconi University.
[1] Matthew Ball, *The Metaverse: And How It Will Revolutionize Everything* (Liveright 2022).

business models in the digital age. As a matter of fact, adopting excessively restrictive approaches as regards the governance of this new technology may have negative effects on its development.
In the contemporary context, it is thus essential to start investigating how the phenomenon of the metaverse should be addressed in the future, taking into account both the opportunities it offers and the constitutional challenges it poses. With this respect, the present work focuses most notably on two areas that most likely will affect the sustainability of platforms' business model in the metaverse in the years to come: that of privacy and data protection; and that of content moderation.

As regards privacy and data protection, the General Data Protection Regulation (GDPR) has only been a first step that underlines the ever-increasing primacy of such rights within the European paradigm.[2] The opinion delivered by Advocate General (AG) Rantos in the case of *Meta Platforms v. Bundeskartellamt*[3] has underlined that the adoption of the legitimate interest as a legal basis to analyse users' personal data for the purposes of advertising may not be justified by a clear and evident necessity of such processing of data, so that additional efforts of the data controller may be required. The decision of the Court of Justice of the European Union (CJEU) confirmed that Meta cannot rely on contractual necessity and the legitimate interest when processing personal data for such purposes.[4] Likewise, this approach has also been confirmed by the recent decisions of the Italian, Spanish, and Irish Data Protection Authorities (DPAs) against TikTok's announcement about a similar shift from consent to legitimate interest for the processing of data for advertising purposes.[5] Both cases are symbolic of the risk that over-enforcement might make the development of digital services in the metaverse at an economic and technological level unsustainable.

At the same time, the protection of freedom of expression, and particularly the rules on content moderation, have also become increasingly fragmented and stringent in

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), O.J. 2016, L 119/1.
[3] CJEU, Case C-252/21, *Meta Platforms, Inc. v. Bundeskartellamt*, Opinion of AG Rantos of 20 September 2022.
[4] Case C-252/21, *Meta Platforms, Inc. v. Bundeskartellamt*, 4 July 2023.
[5] EDPB, 'EDPB adopts letters to Access Now and BEUC on TikTok and an Art. 65 dispute resolution binding decision regarding Instagram' (*EDPB*, 29 July 2002) <https://edpb.europa.eu/news/news/2022/edpb-adopts-letters-access-now-and-beuc-tiktok-and-art-65-dispute-resolution-binding_en>.

the last few years. The Digital Services Act (DSA) is only one examples of the instruments addressing content moderation in Europe. Despite the critical importance of the DSA in providing a new horizontal system of safeguards in content moderation, this instrument may actually influence the evolution of the metaverse,[6] particularly when looking at online advertising. The impact of the DSA is particularly relevant also considering that the regulation of the metaverse does not only involve content moderation but also conduct moderation. Nonetheless, it is evident that the ever-increasing body of laws in the digital field addressing online content will translate into higher compliance costs also for future technologies while making enforcement unpredictable.

This European approach needs to be framed within the landscape of European (digital) constitutionalism,[7] where the concept of proportionality plays a critical role in ensuring a fair balance among conflicting constitutional interests, as particularly underlined by European courts.[8] The European Convention on Human Rights (ECHR) and the Charter of Fundamental Rights of the European Union (CFREU) recognise the possibility that opposing interests, and thus opposing fundamental rights, may enter into conflict: this might be the case, for instance, of the right to freedom of expression and privacy *vis-à-vis* the freedom to conduct business, the latter being protected most notably by Article 16 of the CFREU. In those cases, it is possible for public institutions to decide for the compression of a specific right in favour of other ones, provided that such compression is necessary for the pursuit of the legitimate interest of guaranteeing constitutional values and rights and provided that the measure adopted is proportionate and does not affect the essence, or core, of the fundamental right involved.[9] Besides, both the ECHR and the CFREU provide a limitation to the abuse of rights, thus recognising that the protection of fundamental rights cannot lead to the destruction of other constitutional interests.[10] This constitutional approach underlines the critical role of proportionality in Europe.

---

[6] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ L277/1.

[7] Giovanni De Gregorio, *Digital Constitutionalism in Europe. Reframing Rights and Powers in the Algorithmic Society* (Cambridge University Press 2022).

[8] Oreste Pollicino, *Judicial Protection of Fundamental Rights on the Internet. A Road Towards Digital Constitutionalism?* (Hart 2021).

[9] CFREU, Art 52(1). See Koen Lenaerts, 'Limits on Limitations: The Essence of Fundamental Rights in the EU' (2019) 20 German Law Journal 779; Sébastien Van Drooghenbroeck and Cecilia Rizcallah, 'The ECHR and the Essence of Fundamental Rights: Searching for Sugar in Hot Milk?' (2019) 20 German Law Journal 904.

[10] ECHR, Art 17; CFREU, Art 54.

Against this backdrop, the present work argues that, as the central pillar of European constitutionalism, the principle of proportionality should represent the lodestar guiding the discourse on the metaverse in the EU, with a view to ensuring the protection of fundamental rights and democratic values while avoiding suffocating the creation and development of the metaverse itself. In this case, this work underlines that the risk-based approach expanding in European digital policies constitutes the translation of the principle of proportionality into regulatory instruments. This paper argues that this approach can lead to strike a fair balance among constitutional conflicting interests and promote a sustainable approach for the development of the metaverse in the Digital Single Market.

The first part of this work attempts to describe the concept of the metaverse, as well as the opportunities and challenges this new space will bring for rights and freedoms. The second part explores the challenges raised in the field of privacy and data protection and content moderation in Europe for the sustainability of the business model of platforms, highlighting the risks connected to the potential unsustainability of over-burdening enforcement. The third part argues that the enforcement of rights and freedoms in the metaverse should aim at fostering the balance between fundamental rights interests and market needs, by taking as the ideal principle to follow and enforce that principle of proportionality which is symbolised by the "risk-based approach" in European digital policy.

2. The Rise of the Metaverse: Opportunities and Challenges

The exact definition of the "metaverse" is still developing and seems to encompass a wide-ranging scope of developing technologies, instruments, and spaces. The term itself has been subjected to some critiques.[11] Nonetheless, it is possible to identify some common traits concerning the meaning of this rapidly self-imposing term. The origins of the word come from the 1992 sci-fi novel *Snow Crash* by Neal Stephenson, who portrayed a dystopian society where individuals could access a parallel world created through virtual reality. Coherently, the "metaverse" generally refers to the use of extended reality (XR), including virtual reality (VR), augmented reality (AR), or mixed reality (MR), to build new digital worlds or to merge the physical dimension with the digital dimension. In this sense, "the Metaverse is a post-reality universe, a perpetual and persistent multiuser environment merging physical reality with digital

[11] Alex Wilhelm, 'If Everything Is the Metaverse Then the Metaverse Is Nothing' (*TechCrunch*, 23 April 2022) <https://techcrunch.com/2022/04/23/if-everything-is-the-metaverse-then-the-metaverse-is-nothing/?> accessed 28 July 2023.

virtuality".[12] More specifically, the metaverse is "a new type of Internet application and social form that integrated a variety of new technologies" by providing "an immersive experience based on augmented reality technology, creates a mirror image of the real world based on digital twin technology, builds and economic system based on blockchain technology, and tightly integrated the virtual world and the real world into the economic system, the social system, and the identity system, allowing each user to produce content and edit the world".[13]

The idea of parallel digital universes and dimensions is not at all new: throughout the 2000s and 2010s, a range of massively multiplayer online role-playing games (MMORPGs), such as Roblox, Minecraft, or Fortnite, have been developed and have become popular on a global scale. Another precursor of the contemporary metaverse can certainly be identified in the well-known application Second Life. The concept itself of the "metaverse" was thus, unsurprisingly, well-known and discussed within scholarly and non-scholarly debate during those years. However, such a term exploded in 2020 and, even more, in 2021.[14] Indeed, what has changed since the turn of the millennium is the technological framework, which can today offer brand new opportunities for the development of the metaverse, from 5G to artificial intelligence technologies. Against this background, the possibilities for building new spaces for social interactions and society as a whole have become extraordinary and have knowingly led platforms and digital firms to strongly invest in the development and exploitation of unprecedented new possibilities. This is the case, in particular, of former Facebook, which was accordingly rebranded to Meta in October 2021.

The metaverse promises to bring with it a range of unprecedented benefits for rights and freedoms. For instance, the metaverse could constitute an exciting new tool for the purposes of education: through such technology, a teacher or professor could virtually take their students to witness an ancient emperor's debate or show architectural or geometric principles and postulates in 3D.[15] But the possibilities of

---

[12] Stylianos Mystakidis, 'Metaverse' (2022) 2 Encyclopedia 486, 486.
[13] Huansheng Ning and others, 'A Survey on Metaverse: The State-of-the-Art, Technologies, Applications, and Challenges' (arXiv, 18 November 2021) 1 <http://arxiv.org/abs/2111.09673> accessed 28 July 2023.
[14] Ibid.
[15] Nick Clegg, 'Making the Metaverse: What It Is, How It Will Be Built, and Why It Matters' (*Medium*, 18 May 2022) <https://nickclegg.medium.com/making-the-metaverse-what-it-is-how-it-will-be-built-and-why-it-matters-3710f7570b04> accessed 28 July 2023; Shirin Ghaffary, 'Meta Top Executive Nick Clegg Explains Facebook's Futuristic Plans for the Metaverse' (*Vox*, 1 July 2022) <https://www.vox.com/recode/23189016/metaverse-nick-clegg-mark-zuckerberg-meta-virtual-reality> accessed 28 July 2023.

the metaverse are much wider. In the case of healthcare, for example, the metaverse could in future be used as a safe environment to train students attending medical school. From a cultural and artistic point of view, art exhibitions and/or concerts could take place in the metaverse allowing for wider and even global participation. From an economic and commercial perspective, a new market is developing with respect to the ownership of digital items, including pieces of art, through the resort to non-fungible tokens (NFTs).

At the same time, the development of the metaverse faces a range of constitutional challenges.[16] The first order of issues concerns the need to incentivise the technical evolution of the metaverse in such a way as to guarantee that the benefits it promises can be truly attained and equally distributed across the population. The many opportunities entailed by the notion of the metaverse are still in their infancy and will require high sums of investments in the years to come before they can, in fact, become a reality. It should not come as a surprise if, in May 2022, Mark Zuckerberg admitted to the corporation's shareholders that Meta would be losing significant amounts of money in the next five years and that it may take up to fifteen years to develop some of the technological tools envisaged by the corporation's idea of the metaverse.[17] For instance, one of the current major problems for the development of the metaverse concerns the necessary hardware. VR headsets, essential to be fully immersed within the metaverse, are still rudimentary and uncomfortable: most people experience motion sickness or physical pain when wearing them.[18] Additionally, such hardware is currently still very expensive, hardly making it accessible for the population at large. Other issues concern the interoperability between the many parallel "worlds" which compose the metaverse: this would be important, for instance, for the purposes of ownership and the transferability of NFTs and digital goods from one platform to another. However, such interoperability still represents a challenging task for developers, and a task which may also not always be fully compatible with a platform's economic interests.[19]

---

[16] Mystakidis (n 12).
[17] Rosie Bradbury, 'Mark Zuckerberg Says Meta's Metaverse Project Will Lose "significant" Sums of Money for up to 5 Years' (*Business Insider*, 26 May 2022) <https://www.businessinsider.com/zuckerberg-metaverse-will-lose-significant-money-3-5-years-2022-5> accessed 28 July 2023.
[18] Eric Ravenscraft, 'What Is the Metaverse, Exactly?' (*Wired*, 15 June 2023) <https://www.wired.com/story/what-is-the-metaverse/> accessed 28 July 2023.
[19] Adi Robertson and Jay Peters, 'What Is the Metaverse, and Do I Have to Care?' (*The Verge*, 4 October 2021) <https://www.theverge.com/22701104/metaverse-explained-fortnite-roblox-facebook-horizon> accessed 28 July 2023.

The second set of issues concerns the protection of fundamental rights and democratic values that can be challenged by the metaverse itself. In general, such issues are not at all new and replicate similar problems which arose in the aftermath of the Internet and of the spread of social media and social networks.

First, these issues include increased concerns about the rights to privacy and data protection. Indeed, platforms and providers may acquire further data from users, such as that obtained, for instance, through biometric emotion recognition; additionally, because of the hardware it shall require, the metaverse could further foster surveillance by private economic actors, with additional data being collected and stored within those devices. New data will thus include information about the movements and physical actions of individuals; about neural activity; about the context where people are in (e.g., localisation); about individuals' physiology.[20] The new sets of data collected via the metaverse could, moreover, be used for a variety of reasons, including the prediction of users' identity, behaviour, activity, and emotional state, mainly for the purposes of advertising and micro-targeting. In general, the metaverse will add on a new layer to already existing issues concerning privacy and data protection, including security and integrity of services.[21]

Second, the metaverse is likely to amplify some risks related to the dissemination of harmful or illegal activity and the regime of liability of online platforms. Harmful and illegal conduct within the new spaces may have a different impact with respect to the Internet and social media and may thus require new and/or different forms of intervention. For instance, sexual harassment, such as virtual "groping", has proven to be a particularly relevant problem within the metaverse, causing traumas similar to those following harassment in the physical world.[22] Because of the highly immersive nature of the metaverse as a space for social communications, interactions, and engagement, content moderation will have to deal not simply with written, figurative, and/or audiovisual content, like online platforms in the context of the Web 2.0, but will also have to deal with (admittedly virtual) bodies and actions. Some have even stated that effective content moderation is not even really feasible

[20] Ling Zhu, 'Metaverse: Concepts and Issues for Congress' (Library of Congress Congressional Research Service, 26 August 2022) R47224 <https://sgp.fas.org/crs/misc/R47224.pdf> accessed 28 July 2023.

[21] Bradley Tusk, 'Regulating the Metaverse(s)' (31 January 2022) < https://mirror.xyz/0x81dB200eD62Ce664B911C211b55F836a208Df868/n-8osyXEl8Dzv_qnrBR1ICdxF55zdIMLP6OI3yU9igY> accessed 28 July 2023.

[22] Tanya Basu, 'The Metaverse Has a Groping Problem Already' (*MIT Technology Review*, 16 November 2021) <https://www.technologyreview.com/2021/12/16/1042516/the-metaverse-has-a-groping-problem/> accessed 28 July 2023.

in the context of the metaverse, because of the extraordinary amount of facts, including conducts, taking place within it. Given the role of content moderation within the business model of platforms,[23] this aspect will likely raise critical issues in the future.

These cases show how the business model of platforms is under pressure with the advent of the metaverse. Compliance with a fragmented set of rules inevitably translates into higher costs impacting the economic sustainability of this space. Besides, the issues for sustainability strictly depend not only on the black letter rules of privacy and freedom of expression, but are also deeply influenced by the practical ways in which such law is enforced both by the judiciary and by the relevant administrative authorities across Member States. Interpretation influences the balancing between the various interests at stake: this point will be especially critical in the context of the metaverse in order to allow the development of this new space and of the advantages it may well be capable of bringing with it.

As the next section underlines, the recent approaches in Europe in the cases of data protection and content moderation have already raised questions for the sustainability of platforms in the metaverse, particularly underlining the constitutional tension between the freedom to conduct business and other constitutional values.

3. Platform Sustainability in the Age of the Metaverse

Against this backdrop, the most important challenge is to understand whether and to what extent the legal approach undergone in recent years by European institutions might be consistent with the development on the market of the metaverse or, conversely, how the law, and the way it is enforced, should be rethought in the context of this brand-new paradigm.

The metaverse is characterised by a business model which might be comparable to that of social media and/or social networks, but which differs from the latter under many aspects. For instance, whereas social media and social networks are mainly based on the profiling and micro-targeting of users' data to provide personalised services to advertisers, with a view to making the process of content moderation and curation primarily oriented to advertising revenues, the metaverse will likely generate profit also through other means. Most notably, these means precisely

[23] Tarleton Gillespie, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media* (Yale University Press 2018).

include the sales and exchange of digital goods and services, based on blockchain and NFT technologies.

EU institutions have progressively abandoned their original liberal approach, a relative of the US legal strategies, and have come to adopt an increasingly regulatory and restrictive strategy.[24] Most notably, this change of trajectory is epitomised by EU law on the rights to privacy and data protection, which, in the last twenty years, have come to play such a central role within the European system that some scholars have come to define them as "Europe's First Amendment".[25] The GDPR, in this sense, constitutes the landmark piece of legislation exemplifying the European regulatory trends. At the same time, it is not only the black letter rule of the GDPR that shows a developing interventionist approach within Europe: even more relevant is, in this respect, the way the law itself is interpreted and thus enforced, both by judicial and administrative bodies. National DPAs, for instance, have proven to be particularly stringent in the way they apply the GDPR: an example of this is, for instance, the decision of banning the use in numerous Member States, including Austria, France, and Italy, of Google Analytics, having the latter been recognised as non-compliant with the EU rules on privacy and data protection.[26] Similarly, the reaction to TikTok's decision of shifting from consent to legitimate interest as a legal basis for the analysis of users' personal data for the purposes of personalised advertising is indicative of the trending approach toward privacy dominating the old continent.

Also, the subject of content moderation has gathered increasing attention within the legal framework of the EU, with the progressive enactment of new rules regulating the moderation practices of online platforms. The EU has intervened via the introduction of sectoral reforms and has, subsequently, initiated the adoption procedure for a horizontal revision of the norms governing this area. However, an important role has been played, previously, by the CJEU herself which, through the adoption of some landmark decisions, contributed to making providers of intermediary services more responsible for the items being presented and disseminated via the Internet. Indeed, the judicial activism of the most important judiciary body of the EU has contributed significantly, through the instrument of interpretation (if not manipulation) of the law, to the material creation of additional duties and obligations of online platforms. Once again, the case of content

[24] Giovanni De Gregorio, 'The Rise of Digital Constitutionalism in the European Union' (2021) 19 International Journal of Constitutional Law 41.
[25] Bilyana Petkova, 'Privacy as Europe's First Amendment' (2019) 25 European Law Journal 140.
[26] NOYB, 'UPDATE: Further EU DPA Orders Stop of Google Analytics' (*NOYB*, 5 July 2022) <https://noyb.eu/en/update-further-eu-dpa-orders-stop-google-analytics> accessed 28 July 2023.

moderation shows the importance that enforcement plays in the actual governance of digital technologies and thus on the creation of an economically sustainable environment for businesses.

In general, these cases underline the role of conflicting constitutional interests, thus making the principle of proportionality a critical point of reference for the evolution of the metaverse. Proportionality, as anticipated above, represents the heart of European constitutionalism, since it is the guiding principle orienting the legislative, judicial, and administrative decisions when it comes to the balancing of conflicting positions, interests, and rights. This is essential, especially in the current moment, also to help face and overcome the challenge of fostering innovation and technological development with a view to allowing for the creation of a metaverse truly beneficial and accessible to each and everyone. In this sense, proportionality, although restructured, will have to continue acting as the lodestar of EU regulation, in order to avoid the premature strangling of the metaverse and of the benefits it may entail in the future.

Privacy and Data Protection

The approach adopted in Europe with respect to privacy and data protection raises significant questions with respect to its economic and technological sustainability in the medium-long run, as well as with respect to the protection of rights and values that are equally relevant and important. Namely, the risk inherently connected to the implementation of an excessively restrictive approach could lead to a violation of the freedom to conduct business, protected by the CFREU under Article 16. The current business models of social media platforms, including social networks, is knowingly based precisely on the collection of data and the promotion of advertising, often personalised and customised to users' interests and preferences. The imposition of disproportionate restrictions upon the collection and processing of personal data for such purposes could ultimately lead to suffocating those business models or, at least, to making increasingly costly the provision of their services to European users.

The question of the market sustainability of European policies will be especially critical with respect to the future development of the metaverse. As already underscored, this space will inevitably entail new important challenges for privacy and data protection rights, especially because it will allow the collection of wider sets of personal data. While it will be important to ensure the protection of these fundamental rights, by designing the appropriate corrective measures, it will be nonetheless also essential to guarantee that such measures do not constrain

excessively technological developments. This aspect should not be underestimated, lest the risk of slowing down the building of the digital services, and thus the loss of opportunities that this new technical frontier may be able to offer. In this context, a central role shall be played in particular by the judicial and administrative authorities vested with the duty of enforcing privacy and data protection rights.

In fact, such authorities have in the past proven to favour an interpretation of privacy and data protection law which tends to recognise the importance of those rights over the majority of other interests. Some landmark decision of the CJEU herself, including most notably *Google Spain*,[27] *Digital Rights Ireland*,[28] and the *Schrems* judicial saga[29], are clear examples of this point. These judgments all had to deal with the balancing of privacy with other fundamental rights or public interests, including freedom of expression and information and the fight against terrorism and other "serious crimes".

Besides, national administrative DPAs have also proven to have adopted a similar perspective. This emerges, for instance, from the previously mentioned ban on Google Analytics in a range of Member States, and is also confirmed by a recent episode that concerned the online platform TikTok. In June 2022, TikTok announced a revision of its terms and conditions with respect to privacy and data protection policies in the European Economic Area, UK and Switzerland.[30] As the social network explained, in order to provide its users with advertisement tailored and customised to their specific interests, it collected and processed data concerning both their on-TikTok and their off-TikTok activity: pursuant to the GDPR the legal basis for this type of processing was consent, so that users had to "opt-in" in order to view personalised advertising and could decide in any moment to "opt-out".[31] The announcement stated that TikTok intended to change the legal basis for personalised advertising: instead of relying on consent, TikTok would ground its data collection and processing activities on the different legal basis of its legitimate interests.[32]

---

[27] CJEU, Case C-131/12, *Google Spain*, 13 May 2014.
[28] CJEU, Case C-293/12, *Digital Rights Ireland and others*, 8 April 2014.
[29] CJEU, Case C-498/16, *Schrems I*, 25 January 2018; Case C-311/18, *Schrems II*, 16 July 2020.
[30] 'Changes to personalised advertising on TikTok' (*TikTok*, 8 June 2022) <https://newsroom.tiktok.com/en-eu/changes-personalised-ads-eu> accessed 28 July 2023.
[31] Thus ibid.: "In order to deliver that personalised, just For You advertising, we currently ask your permission to use two main sources of data. The first is data we collect based on your on-TikTok activity, like the accounts you follow, the videos you like and your profile information. The second is data based on your off-TikTok activity, like information that businesses share with us in order to reach potential customers on TikTok. For example, if you sign up for your favourite band's mailing list, they might try and reach you with an ad on TikTok about their upcoming tour".
[32] Article 6(1)(f) GDPR.

This unilateral change in the terms and conditions with respect to privacy met widespread criticism and concerns about the consistency of TikTok's decision with the GDPR.[33] Also in light of the Guidelines 8/2020 on the targeting of social media, version 2.0, of April 13, 2021, of the European Data Protection Board (EDPB),[34] and of the CJEU's decision in *Fashion ID*,[35] the main issue was represented by the legitimacy of grounding data processing for advertising purposes on legitimate interest instead of consent.[36] In July 2022, the Italian DPA thus issued a decision warning the social network that the intended processing would likely infringe national legislation transposing the e-privacy Directive as well as the GDPR.[37] According to the Italian DPA, the processing of data collected from users' personal devices for the purposes of advertising without their consent would be illegal.[38] The Italian DPA's decision was quickly joined by the Irish and Spanish DPAs, ultimately

---

[33] See, *ex multis*, 'Immediately no: TikTok's new personalized ads will jeopardise rights in Europe' (AccessNow, 5 July 2022) <https://www.accessnow.org/immediately-no-tiktoks-personalised-ads-europe/> accessed 28 July 2023.

[34] EDPB, Guidelines 8/2020 on the targeting of social media users, version 2.0 (13 April 2021) <https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf> accessed 28 July 2023.

[35] CJEU, Case C-40/17, *Fashion ID*, 29 July 2019.

[36] Marco Scialdone, 'TikTok's New Policy of Targeting Advertising without Consent Must Be Stopped' (*Euroconsumers*, 22 June 2022) <https://www.euroconsumers.org/opinions/tiktoks-new-policy-of-advertising-without-consent-must-stop> accessed 28 July 2023. According to the Author, in particular, on the one hand provided data (i.e., data that is actively provided directly to the platform by a user, such as their name) can be processed based on the legitimate interest of the social medium concerned only if this is necessary and proportionate (which was not considered to be the case of TikTok; on the other hand, with respect to observed data (i.e., data that is provided via the simple use of the platform, e.g., via likes and comments), often collected through the use of cookies, the EDPB considers that "legitimate interest cannot act as an appropriate basis, as the targeting relies on the monitoring of individuals' behaviour across websites and locations using tracking technologies" (EDPB's Guidelines, para. 77). Moreover, in the latter case, regard should be had to Article 5(3) of the e-privacy Directive (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) O.J. 2002, L201/37). Pursuant to this provision, "the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information […], inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller".

[37] Garante per la Protezione dei Dati Personali, 'Provvedimento del 7 luglio 2022 [9788429]' (*GPDP*, 7 July 2021) <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9788429> accessed 28 July 2023.

[38] Additionally, the decision found that, following the difficulties admittedly encountered by TikTok in implementing age verification techniques, the new policy would likely affect minors as well as adults, thus raising the DPA's preoccupations with respect to the protection of the privacy of underage users.

leading to the platform's decision to suspend the adoption of the new privacy policies.[39]

The decisions of the Italian, Irish, and Spanish DPAs confirm the general attitude of EU and Member States' institutions towards an enforcement of privacy and data protection rights which is almost absolute. Besides, the mistrust of national DPAs toward the processing of personal data for economic purposes by digital platforms also emerges from the upcoming landmark trial before the CJEU which will address the consistency with the GDPR of the "Transparency & Consent Framework" (TCF) developed by IAB Europe, setting privacy standards followed by a wide range of IT Companies and judged as insufficient by 28 EU DPAs.[40]

The debate over the possibility of adopting legitimate interest as the legal ground for the processing of data by online platforms, notably for the purposes of personalised advertising, is also a central aspect of the *Meta Platforms, Inc. v. Bundeskartellamt* case. The case concerned an order issued by the German Federal Cartel Office against Meta, prohibiting the processing of personal data obtained from non-Facebook sources for micro-targeting and advertising purposes as foreseen within Facebook's terms and conditions. According to the Bundeskartellamt, Meta did not comply with the GDPR and the violations of EU privacy law was to be considered the symptom of Meta's abuse of dominance: following this decision, Meta brought an action before the Higher Regional Court in Düsseldorf, which raised a referral for a preliminary ruling of the CJEU. Among the questions of this case, the referring court sought guidance about the legal bases for the processing of personal data, particularly when that processing is necessary to perform a contract as well as when it is necessary for the pursuit of a legitimate interest. Most notably, the AG has not excluded the possibility to rely on the basis of legitimate interest for the purposes of personalised advertising, especially because Recital 47 of the GDPR explicitly recognises data marketing as a legitimate interest of the controller. However, the AG continued: "[W]hen it comes to the necessity of the processing, it is worth noting that the data in question originate from sources outside Facebook. The question therefore arises as to the 'degree of personalisation' of the advertising objectively necessary in

[39] In an update to its decision of July 12, 2022, TikTok declared: "While we engage on the questions from stakeholders about our proposed personalised advertising changes in Europe, we are pausing the introduction of that part of our privacy policy update. We believe that personalised advertising provides the best in-app experience for our community and brings us in line with industry practices, and we look forward to engaging with stakeholders and addressing the concerns".

[40] Irish Council for Civil Liberties, 'Landmark GDPR decision against "consent" spam to be heard at Europe's highest court (ICCL, 7 September 2022) <https://www.iccl.ie/news/landmark-gdpr-decision-against-consent-spam-to-be-heard-at-europes-highest-court/> accessed 28 July 2023.

that respect. As for balancing the interests at stake, consideration should be given to the nature of the legitimate interest in question (in this case, a purely economic interest), as well as the impact of the processing on the user, including his or her reasonable expectations, and to any safeguards put in place by the controller".[41] As a result, following AG Rantos' interpretation, online platforms are subjected to a burden of proof, concerning the necessity of processing, which is rather cumbersome. The CJEU adopted a stricter interpretation, as it limited the use of legitimate interest and contractual necessity as legal bases in this case, thus emphasising the role of consent as legal basis for the processing of personal data for the purposes of targeted advertising.

The way EU and national institutions interpret and apply the GDPR and, generally speaking, privacy and data protection law may have an impact which is rather significant not only in the context of the governance of the Internet, but which may also be particularly relevant with respect to the future development of the metaverse and its deployment in Europe and capable of affecting and influencing the way the metaverse will evolve in the next few years. If, on the one hand, innovation should not lead to neglect the role of fundamental rights, the protection of individuals' privacy rights could translate into an over-compression of freedoms to conduct business within the EU, as well as of those rights, notably freedom of expression, which could be limited themselves by the withdrawal of these private actors from the European market. In other words, if privacy and data protection were to be enforced as absolute rights, they would risk quashing many other fundamental rights protected, amongst others, by the CFREU.

Thus, even if privacy and data protection are extensively protected in Europe, it is necessary to carefully balance these fundamental rights with other constitutional interests. Currently, the constitutional scale between fundamental rights in Europe appears to be tipped in favour of privacy and data protection rights, creating a legal framework which, if not carefully tended to, may be at odds with the principle of proportionality and thus with the overall framework of European constitutionalism.

Content (and Conduct) Moderation

The approach of European institutions in the context of digital services and markets, however, does not deal only with privacy and data protection, but is much wider and

[41] CJEU, *Meta Platforms, Inc. v. Bundeskartellamt*, Opinion of AG Rantos (n 3) 64.

encompasses an ample range of laws and prospective legislation. Among others, the future regulatory framework concerning the digital environment includes the DSA, which will enter into force in 2024 after its twin, the Digital Markets Act (DMA),[42] as well as the Artificial Intelligence Act (AIA).[43] Most notably, the DSA, though addressing a wide range of issues and challenges concerning providers of intermediary services, represents in particular the arriving point of the evolution of Union law with respect to content moderation regulation.

As regards the responsibility of online platforms, the e-Commerce Directive (ECD),[44] which was inspired by the famous US Section 230 of the Communications Decency Act of 1996 (i.e., the "twenty-six words that created the Internet"),[45] introduced in the EU a "safe harbour" system shielding Internet service providers (ISPs) from liability for illegal third-party content.[46] The scope of applicability of the "safe harbour" was progressively restricted, originally through the intervention of the CJEU. Relying on the wording of Recital 42 ECD, which justified the introduction of those rules based on the "mere technical, automatic and passive nature" of the activities operated by providers, the CJEU ruled in *Google France* that those exemptions only applied to intermediaries acting as "neutral actors",[47] clarifying in subsequent decisions what the concepts of neutrality and non-neutrality of platforms entailed:[48] the exercise of forms of control over the content published by third-party users, in other words, may remove service providers from the protection of the safe harbour doctrine, thus giving rise to intermediary liability. Once again, these

---

[42] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) OJ L265/1.

[43] COM(2021)206 final, "Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts". For current text, see <https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2021/0106(COD)&l=en> accessed 28 july 2023.

[44] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), O.J. 2020 L 178/1.

[45] Jeff Kosseff, *The Twenty-Six Words That Created the Internet* (Cornell University Press 2019).

[46] Arts. 12-14 provide that mere conduit, caching, and hosting providers are all exempt from liability for the presence and dissemination of such content through the Internet inasmuch as they comply with a set of rules: most notably, a notice-and-take-down approach was taken with respect to hosting providers.

[47] Joined Cases C–236/08 *Google France SARL and Google Inc. v. Louis Vuitton Malletier SA*, C-237/08 *Google France SARL v. Viaticum SA and Luteciel SARL* and C-238/08 *Google France SARL v. Centre national de recherche en relations humaines (CNRRH) SARL and Others*, 23 March 2010.

[48] See, *ex multis*, CJEU, Case C-324/09 *L'Oréal and Others*, 12 July 2011; Case C-70/10 *Scarlet*, 24 November 2011; Case C-360/10 *SABAM v. Netlog*, 16 February 2012; Joined Cases C-682/18 *Frank Peterson v. Google LLC and Others* and C-683/18 *Elsevier Inc.v.* Cyando, 22 June 2021.

decisions of the CJEU reveal the creative role of the Court and its capability, through the enforcement of the law, of creating new and additional duties affecting the players of the digital market.

Reflecting a similar "constitutional-driven change of heart",[49] the European lawmaker gradually started introducing new legislative acts imposing duties and obligations for online platforms to take action against the presence and spread of illegal user-generated content, including, most notably, the 2018 Recast of the Audiovisual Media Services Directive (AVMSD),[50] the 2019 Digital Single Market Copyright Directive (DSM Copyright Directive),[51] and the 2021 Regulation on Terrorist Content Online (TCO).[52]

The DSA completes this evolution by setting a horizontal regulation for content moderation which shall deeply revise the previous system developed by the ECD. Although, in fact, the tenets of the safe harbour regime are kept alive in the background, the DSA introduces a range of new duties and obligations for ISPs aimed at guaranteeing the construction of a safe online environment. These new rules are scaled based on the nature of the services provided by online intermediaries, as well as on the number of recipients of those services, with duties and obligations that are especially severe and strict for so-called "very large online platforms" (VLOPs) and "very large online search engines" (VLOSEs). These new duties and obligations are meant to help fight, consistently with the European Democracy Action Plan,[53] a range of unwarranted and/or illegal conducts and activities, including among others disinformation and hate speech. With this respect, the new rules require both the introduction of notice-and-take-down mechanisms and procedures, as well as transparency requirements. For instance, online platforms will be required to give

[49] Oreste Pollicino and Giovanni De Gregorio, 'A Constitutional-Driven Change of Heart: ISP Liability and Artificial Intelligence in the Digital Single Market' in Giuliana Ziccardi Capaldo (ed), *The Global Community Yearbook of International Law and Jurisprudence 2018* (Oxford University Press 2019) <https://doi.org/10.1093/oso/9780190072506.003.0011> accessed 28 July 2023.
[50] Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities, O.J. L303/69.
[51] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, O.J. L 130/92.
[52] Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online, O.J. L 172/79.
[53] COM/2020/790 final, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: On the European democracy action plan".

users a great amount of information and details about their advertising systems (e.g., about the identity of the natural or legal person who paid for a specific advertisement or about the way advertising is presented to users).[54] Additionally, VLOPs and VLOSEs will be required to assess the systemic risks entailed by the provision of their services and take the necessary measures to mitigate those risks.[55]

The developing framework on content moderation is focused on the business models characterising current social media and social networks. Nonetheless, such legislation may well have an impact on the metaverse itself. The metaverse has already raised important challenges with respect to conduct in virtual spaces. However, as for the case of privacy and data protection, it is necessary to underline that moderation will have to face issues that are significantly different from the traditional ones characterising online speech and expression. In fact, in the context of the metaverse, it will probably not be possible to speak of "content" moderation but, rather, of "conduct" moderation because users in the metaverse will be able to associate virtual "actions" to the expression of their thoughts and opinions, so that online platforms might have to deal with the need to actively monitor how people will behave in the new virtual world.

In the absence of specific rules that apply to the metaverse, it is evident that a significant role will be played by those judicial and administrative authorities which will be called to interpret the rules introduced by different instruments that regulate content moderation in Europe. The future competent authorities and National Digital Services Coordinators, as well as the future European Board for Digital Services and the Commission will actively contribute to shaping, through their enforcement practices, the legal framework applicable to the metaverse with respect to content (and conduct) moderation, and will thus be the actors responsible for the correct implementation of the principle of proportionality in this field.

4. The Risk-based Approach and the Quest for Proportionality

These challenges raise questions about how to strike a fair balance between fundamental rights in the digital age, including freedom to conduct business. Proportionality is a key requirement and criterion of legitimacy of any regulatory

[54] DSA, Art 26 .
[55] Ibid, Arts 34-35. Joan Barata, 'The Digital Services Act and Its Impact on the Right to Freedom of Expression: Special Focus on Risk Mitigation Obligations' (*DSA Observatory*, 27 July 2021) <https://dsa-observatory.eu/2021/07/27/the-digital-services-act-and-its-impact-on-the-right-to-freedom-of-expression-special-focus-on-risk-mitigation-obligations/> accessed 28 July 2023.

intervention and enforcement aiming at imposing restrictions upon a fundamental right both within the framework of the ECHR and within the framework of the CFREU.[56] Thus, when dealing with a conflict of opposing fundamental rights, both European and national courts, as well as public authorities, are required to operate a balancing test to ensure that none of those rights is subjected to excessive compression.

Within the EU regulatory framework, the principle of proportionality has been internalised and is reflected by the so-called "risk-based regulation". This legislative approach is typical amongst others of recent digital legislative policies, whereby risk assessment becomes the proxy for defining the correct degree of duties and obligations to be imposed on market actors.[57] Being aware of the perils of disproportionate regulatory measures for the well-being of the Digital Single Market, European institutions have made increasing resort to regulatory strategies meant to actually increase flexibility in European digital policies.[58]

In fact, the risk-based approach does not set uniform rules for all regulated actors but is based on a preliminary assessment of the factual risks posed by certain conducts or by the use of certain tools. Following that assessment, the mitigation measures to be adopted to limit the potential downsides of certain activities and/or technologies are identified and implemented. In other words, a differentiated regime of duty and obligations applies, based on concrete risk scores, with the goal, ultimately, of reaching a balance between fundamental rights and the protection of the market: in this sense, the risk-based approach aspires to foster a model of "optimising constitutionalism", seeking to design "optimal" precautions that do not excessively constrain the various actors playing in the market.[59] As a matter of fact, the risk-based approach is characteristic of European regulation both with respect to privacy and data protection and with respect to content moderation.

---

[56] Alec Stone Sweet and Jud Mathews, 'Proportionality Balancing and Global Constitutionalism' (2008) 47 Columbia Journal of Transnational Law 72.
[57] Giovanni De Gregorio and Pietro Dunn, 'The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age' (2022) 59 Common Market Law Review 473.
[58] Raphaël Gellert, *The Risk-Based Approach to Data Protection* (Oxford University Press 2020); Claudia Quelle, 'Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-Based Approach' (2018) 9 European Journal of Risk Regulation 502; Milda Macenaite, 'The "Riskification" of European Data Protection Law through a Two-Fold Shift' (2017) 8 European Journal of Risk Regulation 506; Zohar Efroni, 'The Digital Services Act: Risk-Based Regulation of Online Platforms' (*Internet Policy Review*, 16 November 2021) <https://policyreview.info/articles/news/digital-services-act-risk-based-regulation-online-platforms/1606> accessed 28 July 2023.
[59] Adrian Vermeule, *The Constitution of Risk* (Cambridge University Press 2013) 77.

In the case of data protection, the concept of accountability as defined by the GDPR reflects precisely this new approach to risk, since it leaves data controllers and data processors free to define the measures to be taken to reduce the downsides of processing activities.[60] As a matter of fact the GDPR entrusts data controllers directly with the responsibility of ensuring that the processing of personal data is aligned with the protection of the general principles it sets. Data controllers are required to assessing the risks entailed by their activities and act accordingly. Thus, the way the GDPR rules and principles are declined in practice is mainly up to the targets of regulation, revealing a bottom-up approach toward privacy and data protection that is, in theory, flexible and open to "customisation".

In the case of content moderation, the DSA also follows the strategy of the risk-based approach, though the bottom-up architecture characterising the GDPR seemingly shifts, slightly, towards a more top-down regulatory perspective, thus making way to an "intermediate" structure. The adoption of an "asymmetric"[61] approach, whereby the obligations and due diligence duties of ISPs vary depending on their nature and size, welcomes the principle of proportionality, which represents a key feature of Union risk-based digital regulation, and is the symptom of the will to seek an optimal balancing of democratic values, fundamental rights, and market needs. The main difference between the approach of the GDPR and that of the DSA is that, whereas the former gave a very ample margin of discretion to data controllers and data processors with respect to the mitigation of the measures to put in place, the DSA operates a first risk assessment, identifying the various categories of risk and designating the legal regime applicable to each. Nonetheless, a range of provisions, including the abovementioned rules on the assessment of systemic risks by VLOPs and VLOSEs, confirm the will of the European lawmakers to develop a system which is as flexible as possible.[62]

---

[60] Gellert (n 58).

[61] Joan Barata and others, 'Unravelling the Digital Services Act Package' (European Audiovisual Observatory 2021) 2021–1 <https://rm.coe.int/iris-special-2021-01en-dsa-package/1680a43e45> accessed 28 July 2023.

[62] Besides, the proposed AIA, which will likely affect the development and regula-tion of the metaverse as much as the GDPR and DSA, seems to complete the shift from a bottom-up approach to digital risk-based regulation towards a top-down structure: in fact, the AIA sets four risk categories for AI systems, setting directly, from above, the measures to be actively put in place to reduce the risks those systems entail. Rather than entrusting providers and users of AI systems with the task of developing their own risk mitigation system, the AIA restricts the margins of discretion. Pursuant to the AIA, the assessment of risk is carried out directly by the European Commission, rather than by the targets of regulation itself. De Gregorio and Dunn (n 57); Lilian Edwards,

Be it as it may, the core goal which is infused within these legislative instruments, and which drives (and should drive) risk-based regulation in the digital age, is the fostering of a balanced regime combining both the protection of constitutionally relevant rights and values and the needs of the (digital) market. Indeed, a differentiated legal regime, aimed at avoiding the imposition of unnecessarily strict measures on those activities, conducts, and technologies which prove to be the most innocuous, represents a key declination of the principle of proportionality.[63] Proportionality represents a core value of European constitutionalism, and thus of the developing European digital constitutionalism,[64] and represents the key to the creation of a legal framework capable of tending both at the protection of fundamental democratic values and rights and at the upholding of an environment which is market sustainable. The risk-based approach epitomises the will to build a framework where the various, and sometimes conflicting, interests at stake are consistently balanced and guaranteed at their core.

However, the previous sections have pointed out how the material impact of the law on the balancing of rights and freedoms largely depends upon enforcement practices and upon how the law itself is interpreted and applied. Judicial and administrative authorities have throughout the last decades impacted enormously on the practical developments of privacy and speech governance in Europe. Against this backdrop, the most important challenge will be to understand whether and to what extent the way European institutions will enforce with the protection of fundamental rights and freedoms is consistent with the flexible and proportionality-driven mindset characterising the heart of risk-based regulation, especially with respect to the future governance of the metaverse.

Although the metaverse will be characterised by a business model in some ways comparable to that of social media, it will nonetheless present also features differing significantly from them. It is against this backdrop that the principle of proportionality, interpreted as the guiding parameter of European constitutionalism, will have to play a critical role in the construction of a constitutional framework for the metaverse that strikes a fair balance between innovation and the protection of

---

'Regulating AI in Europe: Four Problems and Four Solutions' (Ada Lovelace Institute 2022) <https://www.adalovelaceinstitute.org/report/regulating-ai-in-europe/> accessed 28 July 2023.

[63] The purpose of deploying a proportionate intervention that does not stifle excessively technological development and the market, was explicitly underscored by the European Commission within the Explanatory Memorandum to the AI Act proposal.

[64] De Gregorio (n 24); De Gregorio (n 7).

fundamental rights and will have to be central in the practices of those who enforce the law of the European Union.

In accordance with the main tenet of the risk-based regulation, characterising, as mentioned above, one of the processes of European digital constitutionalism, proportionality is the keyword driving the discussion on fundamental rights and democratic values in the context of the Digital Single Market, also, and especially, when it comes to the sustainability of social media in the metaverse.

5. Conclusions

The rise of the metaverse will likely revolutionise how individuals experience and enjoy the digital environment and society as a whole. This space could well lead to unprecedented novelties and benefits, though it shall also lead, inevitably, to new challenges and risks. More in general, the metaverse provides an opportunity to stress the role of proportionality up until now in the digital age. This is essential, especially in the current moment, also as a means to help face and overcome the challenge of fostering innovation and technological development with a view to allowing for the creation of a metaverse truly beneficial and accessible to each and everyone.

Technological development, with the advantages and opportunities it can bring, should not be economically unsustainable. The case of TikTok, AG Rantos' opinion for *Meta Platforms*, and the upcoming case concerning IAB Europe's TCF showcase precisely how legislation, even when legitimately seeking to further fundamental rights, might affect in a disproportionate way the providers of digital services. Also with respect to content/conduct moderation, it will be critical for European and Member States' institutions to focus on guaranteeing a proportionate framework taking into account both the needs of the market and technological innovation and the specific aspects characterising the metaverse, as opposed to the different business model of online social media.

To this regard, a critical role is played not only by lawmakers, but also by those who interpret it, apply it, and enforce it. Disproportionate approaches could easily become unsustainable vis-à-vis the promotion of interests that are fundamental for the EU itself: most notably, the creation of a competitive and sound Digital Single Market and the protection of fundamental rights. As a matter of fact, the enforcement of privacy and data protection law, as well as of content moderation regulation would benefit from a cooperative approach, taking into account that existing law, such as, notably, the GDPR, already sets important constraints protective of individual rights.

In this sense, public EU and national institutions could fall into the trap of assuming, as a prejudice, the companies' failure to comply with the requirements and principles connected to EU digital laws and policies.

Overall, the principle of proportionality is the lodestar to guide the evolution of the metaverse. Particularly, the risk-based approach to regulation, which, even though through the adoption of different forms, has become more and more popular in the last decades, reflects precisely the aspiration to pursue a balance between the various interests at stake. Proportionality will thus have to ensure, especially, that regulatory and enforcement duties and costs do not excessively encumber the market players dedicated to the development of the metaverse. This will be essential to ensure the creation of a sustainable space where everyone may enjoy the opportunities of digital technologies, including those offered by the metaverse.