# GDPR IN A METAVERSAL POST-DIGITAL WORLD: THE LAW OF EVERYTHING OR THE LAW OF NOTHING?

**by *Cyril Fischer***

**ABSTRACT:** This article critically examines whether the General Data Protection Regulation (GDPR), presented as technologically neutral, provides a robust framework for the metaverse. The article critically assesses the GDPR as the 'law of everything', arguing that the GDPR applies too broadly, before addressing the counterargument of the GDPR as the 'law of nothing', whereby the GDPR fails to protect data subjects against the processing of their emotion or mental data. The article presents a critical evaluation of the traditional approach consisting in the creation of novel rights. It rather proposes a top-down approach whereby the EU lawmaker would forbid the processing of emotion and mental data for commercial purposes. Additionally, it proposes a redefinition of the material scope of the GDPR to address the pitfalls arising from the GDPR as the 'law of everything' and the 'law of nothing'.



## 1 Introduction

Coined in 1992 by Neal Stephenson in the novel 'Snow Crash'[1], the metaverse's hype reached its climax when the social media company 'Facebook' became 'Meta' in 2021 to proclaim its strategy and vision for the future: the metaverse.[2] The hype did however not last long, as Meta's stock value was divided by four around one year later, and Reality Labs (Meta's metaverse division) announced severe losses and layoffs.[3]

[1] Neal Stephenson, *Snow Crash* (Bantam 1992) 440.

[2] Meta, 'Introduction Meta: A Social Technology Company' <https://about.fb.com/news/2021/10/facebook-company-is-now-meta/> accessed 24 October 2024.

[3] Steve Rose, '"The Metaverse Will Be Our Slow Death!" Is Facebook Losing Its $100bn Gamble on Virtual Reality?' *The Guardian* (7 December 2022) <https://www.theguardian.com/technology/2022/dec/07/metaverse-slow-death-facebook-losing-100bn-gamble-virtual-reality-mark-zuckerberg> accessed 24 October 2025.

Since these dark hours for Meta, its stock value was multiplied by eight at the time of writing this article and, together with other big tech companies (eg Apple with the Apple Vision Pro), it continuously develops and markets new metaverse technologies.[4]

Conscious of the fact that the metaverse has not reached mass adoption yet, but is poised to become a 'ground-breaking'[5] technology - with a market size that could be multiplied by around thirty in eight years according to Bloomberg[6] – the European Commission has adopted in 2023 a strategy for the metaverse (which it calls the Web 4.0, as discussed below).[7] Since 2023, the European Commission – together with the European Parliament[8] and the Council of the European Union[9] – has been working on the metaverse.

While the European Parliament[10] and the Council of the European Union[11] call for a reform of the General Data Protection Regulation[12] ('GDPR'), the European Commission adopts a more conservative stand, as it seems to consider that the GDPR, allegedly being 'technologically neutral'[13], 'also fully applies to the processing of

[4] Hortense Goulard, 'Le métavers à la relance' (*Les Echos*, 6 February 2024) <https://www.lesechos.fr/idees-debats/editos-analyses/le-metavers-a-la-relance-2074303> accessed 24 October 2025; Dèbes Florian, 'Mark Zuckerberg, l'aventurier tenace du métavers et des mondes virtuels' (*Les Echos*, 28 September 2024) <https://www.lesechos.fr/tech-medias/hightech/mark-zuckerberg-laventurier-tenace-du-metavers-et-des-mondes-virtuels-2121928> accessed 24 October 2025.

[5] Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Long-term competitiveness of the EU: looking beyond 2030' (Communication) COM(2023) 168 final.

[6] Commission, 'Commission Staff Working Document Accompanying the document: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: An EU initiative on Web 4.0 and virtual worlds: a head start in the next technological transition' SWD(2023) 250 final 11.

[7] Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: An EU initiative on Web 4.0 and virtual worlds: a head start in the next technological Transition' (Communication) COM(2023) 442 final; Commission, 'Commission Staff Working Document Accompanying the document: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: An EU initiative on Web 4.0 and virtual worlds: a head start in the next technological transition' SWD(2023) 250 final.

[8] Tambiama Madiega, Polna Car and Maria Niestadt, 'Metaverse: Opportunities, risks and policy implications' (European Parliament, 2022) < https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733557> accessed 13 January 2023; Mariusz Maciejewski, 'Metaverse' (European Parliament, 2023) < https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2023)751222> accessed on 20 October 2023.

[9] Council of the European Union, *'Metaverse: Virtual World, Real Challenges'* (2023) <https://data.europa.eu/doi/10.2860/432862> accessed 13 January 2023.

[10] Madiega, Car and Niestadt (n 8) 6.

[11] Council of the European Union (n 9) 10.

[12] 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) [2016], OJ L119/1.

[13] See also Recital 15 of the GDPR.

personal data in virtual worlds'.[14] With the latest 'GDPR Omnibus'[15] proposal, it seems that the European Commission does not consider a reform of the GDPR in light of the metaverse.[16]

## 1.1 Aim of the Research

Against that background, this paper will analyse and assess the extent to which the GDPR indeed remains a sound framework when applied to the metaverse, in particular in light of its core values and objectives.

This paper only focusses on the GDPR, and excludes other legal frameworks that might directly or indirectly regulate the data processing activities that will occur in the metaverse, such as the AI Act[17], the Digital Services Act[18], or the Digital Markets Act[19].

To frame that analysis, it is necessary to clarify the metaverse concept - as well as the data processing activities that would typically occur in the metaverse – and the core values the GDPR aims to safeguard.

## 1.2 Framing the Metaverse Concept

Matthew Ball's seminal work[20] offers a useful definition of the metaverse. According to Ball, the metaverse is the following:

[14] COM(2023) 442 (n 7) 5.
[15] Commission, 'Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2016/1036, (EU) 2016/1037, (EU) 2017/1129, (EU) 2023/1542 and (EU) 2024/573 as regards the extension of certain mitigating measures available for small and medium sized enterprises to small mid-cap enterprises and further simplification measures' COM(2025) 501 final/2 (GDPR Omnibus).
[16] Christopher Kuner, 'The Draghi Dilemma: The Right and the Wrong Way to Undertake GDPR Reform' (Future of Privacy Forum, 23 October 2025) <https://fpf.org/blog/the-draghi-dilemma-the-right-and-the-wrong-way-to-undertake-gdpr-reform/> accessed 27 October 2025.
[17] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) [2024], OJ L.
[18] 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) [2022], OJ L277/1.
[19] 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) [2022] OJ L265/1.
[20] Matthew Ball, *The Metaverse: And How It Will Revolutionize Everything* (Liveright 2022).

> [A] massively scaled and interoperable network of real-time rendered 3D virtual worlds that can be experienced synchronously and persistently by an effectively unlimited number of users with an individual sense of presence, and with continuity of data, such as identity, history, entitlements, objects, communications, and payments.[21]

The European Commission also provides a definition of the metaverse, which it calls the 'Web 4.0', as the successor of the Web 3.0 (the decentralised web) and of the Web 2.0 (the web of the social media and user generated content):

> Web 4.0 is the expected fourth generation of the World Wide Web. Using advanced artificial and ambient intelligence, the internet of things, trusted blockchain transactions, virtual worlds and XR capabilities, digital and real objects and environments are fully integrated and communicate with each other, enabling truly intuitive, immersive experiences, seamlessly blending the physical and digital worlds.[22]

The key feature of the metaverse that is common to these two definitions is its immersive nature, or what Ball calls the 'sense of presence'. True immersion will only become possible through the use of novel interfaces, shifting from traditional computers, (smart) phones and tablets to glasses, headsets, or haptic wearables.[23]

The purpose of those new technologies is that when users act in the physical world (the 'real' world), their actions (body movements, voice, pupil movements, gaze, gait, etc.[24]) should also be displayed in or influence the metaverse.[25] To put it simply, if someone jumps or smiles, his or her avatar in the metaverse should also be jumping or smiling. This is a major difference with Web 2.0 or Web 3.0, as with the metaverse, real world data will also be massively processed via sensors, in addition to the data processing activities that will occur in the digital world (which already exist in the Web 2.0 or Web 3.0). It is against that background that one considers that the metaverse is an 'always-on recording'[26] system that will lead to a fusion of the physical and the

[21] ibid 29.
[22] SWD(2023) 250 final (n 7) 1-2.
[23] ibid 48; Adrien Basdevant, Camille François and Rémi Ronfard, 'Mission exploratoire sur les métavers' (October 2022) 35 <https://www.economie.gouv.fr/files/files/2022/Rapport-interministeriel-metavers.pdf> accessed 7 June 2023.
[24] Ben Egliston and Marcus Carter, 'Critical Questions for Facebook's Virtual Reality: Data, Power and the Metaverse' (2021) 10 Internet Policy Review <https://policyreview.info/articles/analysis/critical-questions-facebooks-virtual-reality-data-power-and-metaverse> accessed 28 October 2025; Elizabeth M Renieris, *Beyond Data: Reclaiming Human Rights at the Dawn of the Metaverse* (The MIT Press 2023) 154–155; Mark McGill, 'The IEEE Global Initiative on Ethics of Extended Reality (XR) Report–Extended Reality (XR) and the Erosion of Anonymity and Privacy' (*IEEE*, November 2021) 7 <https://ieeexplore.ieee.org/document/9619999> accessed 28 October 2025.
[25] Ryan Calo and others, 'Augmented Reality: A Technology and Policy Primer' [2016] Tech Policy Lab 3–4 <https://digitalcommons.law.uw.edu/techlab/1>; Egliston and Carter (n 24); McGill (n 24) 7.
[26] Calo and others (n 25) 6.

virtual worlds. As the European Commission puts it, 'digital and real objects and environments are fully integrated and communicate with each other, (…) seamlessly blending the physical and digital worlds.'[27] In a world where the physical (offline) and the digital (online) are blended, where there is 'internet in everything'[28], the notion of digital has become archaic: this is the advent of the so-called 'post-digital' world.[29]

## 1.3 GDPR: Core Objectives

At its core, the GDPR aims at protecting the personal data of natural persons and at realising the fundamental right to data protection, which is enshrined in Articles 8(1) of the Charter of Fundamental Rights of the European Union[30] and 16(1) of the Treaty on the Functioning of the European Union[31] (TFEU).[32]

However, the GDPR is not limited to the protection of personal data. Indeed, it also serves as a cornerstone for other rights, such as the principle of informational self-determination, autonomy, human dignity and control.[33] For the purpose of this article, we understand the principle of informational self-determination as 'the capacity of the individual to determine in principle the disclosure and use of his/her personal data'.[34] As a right to decide for oneself in the context of the processing of personal data, the principle of informational self-determination is deeply connected to the principles of autonomy and control. Autonomy can be understood as the capacity to make one's own decisions and to be in control (positive aspect), which also entails a negative aspect (a freedom from external constraint).[35] Human dignity can be

[27] SWD(2023) 250 final (n 7) 1-2.
[28] Laura DeNardis, *The Internet in Everything: Freedom and Security in a World with No Off Switch* (Yale University Press 2020).
[29] Renieris (n 24) 99. For the concept of the 'post-digital' era, see Accenture's report: Accenture, 'The Post-Digital Era is Upon Us: Are You Ready For What's Next?' (2019) <https://www.accenture.com/content/dam/accenture/final/a-com-migration/r3-additional-pages-1/pdf/pdf-94/accenture-techvision-2019-exec-summary.pdf> accessed 12 November 2025.
[30] Charter of Fundamental Rights of the European Union, OJ 2010 C 83/389.
[31] Consolidated Version of the Treaty on the Functioning of the European Union [2016] OJ C 202/1.
[32] Recital 1 of the GDPR.
[33] Tommaso Fia, 'Fairness in Market Instrumental Data Law' (2025) 33 International Journal of Law and Information Technology 4; Paul Friedl, *Reasonable Expectations of Privacy: With Special Regard to European Privacy and Data Protection Law* (1st ed. 2025, Springer Nature Switzerland 2025) 299–301; Nadezhda Purtova, 'Default Entitlements in Personal Data in the Proposed Regulation: Informational Self-Determination off the Table … and Back on Again?' (2014) 30 Computer law & security review 6; Damian Clifford, *Data Protection Law and Emotion* (1st edn, Oxford University Press 2024) 185.
[34] Paul De Hert and Serge Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer 2009) 14.
[35] Nita A Farahany, *The Battle for Your Brain: Defending the Right to Think Freely in the Age of Neurotechnology* (First edition, St Martin's Press 2023) 119. For a thorough analysis of the concept of autonomy, see Dworkin's seminal work: Gerald Dworkin, *The Theory and Practice of Autonomy* (Cambridge University Press 1988).

understood as the right to be respected (which includes a right to autonomy).[36] Finally, in the context of data protection, Bygrave defines control as the ability 'to participate in, and have a measure of influence over, the processing of data on them by other individuals or organizations'.[37]

### 1.4 Structure of the Research

This paper first critically assesses the GDPR as the 'law of everything', ie the argument that the GDPR applies too broadly (Section 1). It subsequently addresses the counterargument – which we call the GDPR as the 'law of nothing' – ie the conclusion that the GDPR fails to protect data subjects against the processing of their emotion or mental data (Section 2). We structure each section in the same way, starting with the relevant data processing activities at hand, to subsequently identify the problems these activities pose for the GDPR. Somewhat paradoxically, both claims - that the GDPR is the 'law of everything' and 'of nothing' - show the limits and problems the GDPR would generate in a metaversal context, but also in its current application.

Confronted with those findings, the third section of the paper identifies and conceptualises solutions to the problems identified under sections 1 and 2. More particularly, we will present how the GDPR's core could be enhanced to address both the 'law of everything' and the 'law of nothing' critiques.

## 2 GDPR as the 'Law of Everything'

### 2.1 Metaversal Data Processing Activities: the Quantitative Problem

Akin to what the web users experience today, the users' activities in the digital world (the web of today, or the metaverse of tomorrow) will often be tracked, leading to massive online data processing activities. Similar data tracking will take place in the metaverse as well.

In terms of the quantity of the data processing activities, the paradigm shift lies above all elsewhere: not in the digital world, but in the physical world. Indeed, the

[36] Marcus Düwell, 'Human Dignity and the Ethics and Regulation of Technology' in Roger Brownsword, Eloise Scotford and Karen Yeung (eds), *The Oxford Handbook of Law, Regulation and Technology*, vol 1 (Oxford University Press 2017) 185–186.
[37] Lee A Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits* (Wolters Kluwer Law International 2002) 63.

metaversal interfaces will bear sensors, which will massively process real world data to influence the digital world. This is characteristic of the 'always-on recording' system as highlighted in our description of the metaverse.[38] When the physical and the digital world are blended, everything becomes data[39] and could easily become personal if the broad requirements of Article 4(1) of the GDPR are met.[40]

## 2.2 The Quantitative Problem and the GDPR

In 2018, Purtova already warned against the consequences of the GDPR being applied too broadly and thus becoming the 'law of everything'.[41]

Even though the GDPR as the 'law of everything' might seem appealing at first sight – to the extent that it would offer a broad protection to data subjects on paper, it would actually lead to or even further aggravate two core pitfalls in the GDPR and its implementation.

### 2.2.1 Two Pitfalls of the GDPR as a Result of the Law of Everything

First, it may lead to a 'system overload'[42] for controllers and processors - who are bound to respect a strict framework of obligations (with potentially severe sanctions[43]) – on the one hand, and for data protection authorities – who must supervise and enforce the GDPR - on the other hand. With regard to the controllers and processors, as Purtova puts it, the system overload will harm meaningful compliance.[44] Controllers and processors might thus choose to simply refrain from processing personal data (which would be against one of the core objectives of the GDPR - ie to allow for the free movement of personal data[45] - and would prevent positive externalities of the use of personal data, such as in the health sector), or to put priorities to compliance activities (potentially thus parking or excluding compliance for

[38] See our description of the metaverse in the introduction. See also Calo and others (n 25) 3-4,6; McGill (n 24) 7; Egliston and Carter (n 24).
[39] Renieris (n 24) 113; Nadezhda Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10 Law, Innovation and Technology 40, 2.
[40] Vasilis Xynogalas and Mark Leiser, 'The Metaverse: Searching for Compliance with the General Data Protection Regulation' (2024) 14 International Data Privacy Law 89, 102.
[41] Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (n 39).
[42] ibid.
[43] See Art. 84 GDPR.
[44] Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (n 39) 30–33.
[45] See Art. 1(1) GDPR.

activities with lower risks), or to undertake compliance as a purely formal exercise, leading to a 'formal appearance of compliance'[46] instead of meaningful material compliance. Finally, with regard to data protection authorities, there is already sufficient research demonstrating that enforcement is complicated and not necessarily fully effective today, amongst others because of the mismatch between the number of cases and the resources such authorities have.[47] The rise of the metaverse could further exacerbate the gap and thus, the malfunction of enforcement.

Second, the 'law of everything' would also be problematic for data subjects. This might seem counterintuitive, as the GDPR grants rights to data subjects. While it is easy to understand the problems controller and processors face when they have too many obligations, how can there be too many rights for data subjects? These rights were conferred on data subjects to provide them with control over their personal data.[48] The problem with individual control is that it is not scalable.[49] While it would seem appropriate to ask individuals to carefully review and control key contractual terms (such as the purchase agreement of their house or their marriage contract), individuals cannot seriously be expected to control several privacy and contractual terms on a daily basis.[50] Once a certain threshold is crossed – which we have long passed in Western society[51] – control becomes a mere 'fantasy'[52], an 'illusion'[53] or a legal fiction to have a normative ground for mechanisms that are known to fail.[54] As McGill nicely puts it, when consent is sought in the metaverse – consent being one of

[46] Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (n 39) 32.
[47] Brave, 'Europe's governments are failing the GDPR. Brave's 2020 report on the enforcement capacity of data protection authorities' (2020) < https://brave.com/blog/dpa-report-2020/> accessed 30 October 2025; Lokke Moerel, 'Metaverse and Data Protection' in Larry A DiMatteo and Michel Cannarsa (eds), *Research Handbook on the Metaverse and Law* (Edward Elgar Publishing 2024) 154.
[48] See Recital 7 of the GDPR and our footnote 33.
[49] Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (Harvard University Press 2018) 64; Cass R Sunstein, *The Ethics of Influence: Government in the Age of Behavioral Science* (Cambridge University Press 2016) 65 <https://www.cambridge.org/core/books/ethics-of-influence/E29EDE19EBCB53F6D8691730668115F7> accessed 30 October 2025.
[50] Aleecia M McDonald and Lorrie Faith Cranor, 'The Cost of Reading Privacy Policies'(2008) 4 A Journal of Law and Policy for the Information Society 543; Pierre-Nicolas Schwab, 'Reading Privacy Policies of the 20 Most-Used Mobile Apps Takes 6h40' (*Into the Minds*, 28 May 2018) <https://www.intotheminds.com/blog/en/reading-privacy-policies-of-the-20-most-used-mobile-apps-takes-6h40/> accessed 30 October 2025.
[51] See footnote 50.
[52] Renieris (n 24) 64.
[53] Neil M Richards and Woodrow Hartzog, 'Taking Trust Seriously in Privacy Law' (2016) 19 Stanford Technology Law Review 431.
[54] Renieris (n 24) 64, 71; Alicia Solow-Niederman, 'Information Privacy and the Inference Economy' (2022) 117 Northwestern University Law Review 357, 364; Jamie Susskind, *The Digital Republic: Taking Back Control of Technology* (Bloomsbury Publishing 2023) 105–112.

the cornerstone of the control allegedly provided by the GDPR[55] – it often leads to a 'consensual erosion of rights'.[56]

The 'law of everything' problem exposes the unsuitable character of the GDPR to achieve its core objectives. Indeed, the rights and interests to data protection, informational self-determination, autonomy, human dignity and control for data subjects would only benefit from an illusion of protection that cannot be seriously exercised. This, in turn, poses another challenge to the right to human dignity understood as the right to be respected.[57]

### 2.2.2 GDPR Obsolecence

The 'law of everything' problem of the GDPR reveals its obsolescence and the fact that it will not resist well to the metaverse, even though it was presented as technologically neutral.[58] A brief historical outlook on the GDPR's genesis confirms that finding. The sociotechnological context in which the core principles of the GDPR were adopted was very different from today's and tomorrow's environment. Indeed, the core principles of the GDPR (lawfulness, fairness, transparency, purpose limitation, storage limitation, data minimisation, accuracy, integrity and confidentiality, accountability) date back from the Fair Information Practices Principles (FIPPs) adopted back in the 70s and 80s.[59] At that time, it was the very start of personal computers and the key technologies behind internet (TCP/IP, HTML and URL) saw the light of day. However, it is only one decade later (in the 90s) that internet really started to reach mass adoption.[60] The years 2000 saw the outbreak of smart phones and the Web 2.0 (social media and user-generated content). In the present article, we are discussing a technology that promises to significantly emerge in the 2020s or 2030s.[61] Thus, the GDPR core principles have hardly changed, while the world has known major disruptions (internet, smart phones and the Web 2.0).

These disruptions are not only technological, they are also and mostly relational.[62] In the 70s and 80s, the first data protection frameworks were adopted as

[55] Hartzog (n 49) 63; Richards and Hartzog (n 53) 444; Daniel J Solove, 'Introduction: Privacy Self-Management and the Consent Dilemma' (2013) 126 Harvard law review 1880, 1880; Neil Richards and Woodrow Hartzog, 'The Pathologies of Digital Consent' (2019) 96 Washington University Law Review 1461, 1472.
[56] McGill, Mark (n 20) 17.
[57] Düwell (n 36) 185–186.
[58] Recital 15 of the GDPR.
[59] Renieris (n 24) 40, 50.
[60] ibid 36–38.
[61] SWD(2023) 250 final (n 7) 11, 32.
[62] Tjerk Timan, Maša Galič and Bert-Jaap Koops, 'Surveillance Theory and Its Implications for Law' in Roger Brownsword, Eloise Scotford and Karen Yeung (eds), *The Oxford Handbook of Law, Regulation and Technology* (Oxford University Press 2017) 732.

safeguards against state databases and interferences ('big brother').[63] Back then, the relationship was bi-directional (state-citizen).[64] For a few decades now, the relationship is multi-directional: data protection no longer serves only as a shield against state interferences, it also protects citizen against interferences from private companies, organisations, and even fellow citizen.[65] As Susskind nicely puts it, big brother gave way to a 'big brotherhood'.[66]

Against that background, the evolution of data protection into the 'law of everything' becomes more comprehensible. Even though the GDPR obligations and rights were possibly judicious back in the 70s or 80s (eg the transparency and consent framework seemed possible to implement in a one-to-one relationship), they are less so today, and even lesser so tomorrow.

# 3 GDPR as the Law of Nothing

## 3.1 Metaversal Data Processing Activities: the Qualitative Problem

As explained above, the immersive nature of the metaverse - the real 'sense of presence'[67] or embodiment in the digital world – requires the processing of physical world actions (body movements, voice, pupil movements, gaze, gait, etc) to subsequently replicate them in the digital world, eg via the avatar.[68] This phenomenon could quickly lead to the processing of emotion, mind and mental data, including for pure marketing purposes, such as emotional marketing.[69] Meta and Spotify did not hide their intention to do so.[70]

Renieris explains the shift from Web 2.0 to the metaverse very clearly: '[i]f these Web2 platforms sought to datafy *outward* expressions of our personality or relationships, Web3 or metaversal technologies seek to datafy everything, including our external and *internal* physiological, psychological, cognitive, and emotional states.'[71]

[63] Renieris (n 24) 23.
[64] ibid 36.
[65] Timan, Galič and Koops (n 62).
[66] Susskind (n 54) 41.
[67] Ball (n 20) 29.
[68] Basdevant, François and Ronfard (n 23) 42; Andrew McStay, 'Emotional AI, Soft Biometrics and the Surveillance of Emotional Life: An Unusual Consensus on Privacy' (2020) 7 Big Data & Society 2.
[69] Basdevant, François and Ronfard (n 23) 86, 89; Madiega, Car and Niestadt (n 8) 4-5; Renieris (n 24) 101-103; McGill (n 20) 9-11; Moerel (n 47) 126-17.
[70] Renieris (n 24) 101; Xynogalas and Leiser (n 40) 96.
[71] Renieris (n 24) 128.

In addition, the processing or individuals' emotions could – technically speaking – perfectly happen without the identification of concrete individuals.[72] For instance, Häuselmann mentions a billboard from the company Landsec installed at Piccadilly Circus (London) which uses affecting computing[73] and facial detection (not to be confused with facial recognition[74]) to display advertisements based on various inputs, including the mood of passers-by. This process would however exclude any storage of the individuals' faces and any attempt of identifying or singling out individuals.[75] In the same vein, the Italian data protection authority (the *Garante per la protezione dei dati personali*) had to rule on the use of a camera system within an Italian museum to asses how visitors react to paintings (what is the path they use, their state of mind, gender, age group, how long do they stay in front of the painting, etc.). Here again, the system relied on face detection technology.

## 3.2 The Qualitative Problem and the GDPR

The above-described processing of emotions reveals two gaps in the GDPR, ie the qualification of emotion and mental data, and the identification requirement. In turn, these gaps again indicate that the GDPR fails to safeguard its core values and objectives. This is particularly salient given the protection of emotion and mental data is fundamental to the right to freely decide for oneself.

### 3.2.1 Qualification of Emotion and Mental Data under the GDPR

Under the GDPR, emotions and mental data are not as such considered sensitive data in the sense of Article 9 of the GDPR. Indeed, Article 9 exhaustively[76] lists the personal data considered sensitive. These are:

[72] ibid 119–121; McStay (n 68); Andreas Häuselmann, 'Fit for Purpose? Affective Computing Meets EU Data Protection Law' (2021) 11 International Data Privacy Law 245, 248; Garante per la protezione dei dati personali (9896808, 2023).

[73] According to Ienca and Malgieri, affective computing (also known as 'emotion AI') could be defined as the use of computing (often machine learning) to 'detect, interpret, process, and simulate human affects and emotions'. See Marcello Ienca and Gianclaudio Malgieri, 'Mental Data Protection and the GDPR' (2022) 9 Journal of Law and the Biosciences 3.

[74] While facial recognition technology compares an individual's face to a facial template to identify a person, facial detection technology merely detects the presence of a human face, without trying to identify who it is. See Nadezhda Purtova, 'From Knowing by Name to Targeting: The Meaning of Identification under the GDPR' (2022) 12 International Data Privacy Law 163, 164.

[75] Häuselmann (n 72) 248–249.

[76] Ludmila Georgieva and Christopher Kuner, 'Article 9 Processing of Special Categories of Personal Data' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR)* (Oxford University Press 2020) 373.

> 'data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation'.

The qualification of emotion and mental data as non-sensitive personal data may seem counterintuitive, since emotions and thoughts are, in essence, among the most intimate and sensitive information about people.[77] As Ienca and Malgieri aptly put it:

> 'mental representations (and their underlying brain activity) are the closest psychological (and neurobiological) substrate of fundamental ethical-legal notions such as personal identity, personal autonomy, freedom of thought, mental integrity, and others.'[78]

This normative (absence of) choice from the EU lawmaker is even more intriguing, given that the right to freedom of thought is one of the few fundamental rights that benefit from an absolute protection.[79] As its scope is still debated[80] and since it was adopted long before the popularisation of artificial intelligence and the metaverse, it would have deserved to be debated in the context of Article 9 of the GDPR – *quod non*.

Notwithstanding the absence of emotion and mental data in Article 9 of the GDPR, such data may still benefit from an *indirect* protection by Article 9. That would be the case if personal data protected by Article 9 is processed to infer emotion or mental data, eg the processing of biometric data (such as face recognition) or health data (heart rate or blood pressure) to infer stress or anger. This conclusion must however be nuanced with regard to the use of biometric data, which are only sensitive (and thus covered by Article 9 of the GDPR) if they are processed 'for the purpose of uniquely identifying a natural person'.[81] For example, if pupil movements are not processed to uniquely identify someone, but to infer stress patterns, this data processing activity would not benefit from the protection of Article 9 of the GDPR.[82] It should also be emphasised that it is perfectly possible to process emotion and mental data without processing biometric or health data. For instance, the speed of keyboard

[77] Ienca and Malgieri (n 73) 10.
[78] ibid 6.
[79] Farahany (n 35) 188; Renieris (n 24) 164; Taimur Aimen, 'Cognitive Freedom and Legal Accountability: Rethinking the EU AI Act's Theoretical Approach to Manipulative AI as Unacceptable Risk' (2025) 1 Cambridge Forum on AI: Law and Governance e20, 3.
[80] Aimen (n 79) 4.
[81] Article 9(1) of the GDPR.
[82] Häuselmann (n 72) 249–250; Ienca and Malgieri (n 73) 7–11.

typing or of movements (which Ienca and Malgieri call 'behavioural data'[83]) might reveal the level of stress.

The above developments do not entail that emotion and mental data can be freely processed, used and sold. Indeed, to the extent that emotion and mental data qualify as personal data (see below, the second gap of the GDPR), they would be protected by the standard principles and obligations of the GDPR, including the principles of lawfulness, fairness, transparency, purpose limitation and data minimisation enshrined in Article 5(1) of the GDPR. The main difference between the qualification of emotion and mental data as sensitive personal data or as 'regular' personal data lies in the principle of lawfulness, which sets a higher threshold for sensitive data (for which a lawful basis must be found in Articles 9 and 6 of the GDPR[84], the bases of Article 9 being restrictive) than for 'regular' personal data (for which a lawful basis under Article 6 of the GDPR suffices).

### 3.2.2 The Identification Requirement under the GDPR

Pursuant to its Article 2(1), the GDPR only applies to the processing of personal data. Personal data is defined as 'any information relating to an identified or identifiable natural person'.[85] This definition can be broken down into four cumulative requirements: (1) any information; (2) relating to; (3) a natural person; (4) who is identified or identifiable.[86]

The first three requirements have not sparked much controversy within legal scholarship or case law. However, the fourth requirement remains highly controversial, even though the definition of personal data already exists since the data protection directive[87], ie since three decades.[88] The controversy and doctrinal discussions have however focussed on the identifiability criterion, rather than on the identification criterion.[89] Thus, although fundamental, the concept of identification remains ambiguous. According to the Article 29 Working Party – the advisory authority set up by the data protection directive, and which has been replaced by the European Data Protection Board – identification means singling someone out, ie to distinguish someone from other persons.[90] It is unclear whether the case law of the Court of

[83] Ienca and Malgieri (n 73) 5.
[84] Georgieva and Kuner (n 76) 376.
[85] Article 4(1) of the GDPR.
[86] Article 29 Working Party, 'Opinion 4/2007 on the concept of personal data' (WP 136, 20 June 2007) 6.
[87] Directive (EC) 95/46 of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995], OJ L281.
[88] Purtova, 'From Knowing by Name to Targeting' (n 74).
[89] ibid.
[90] Article 29 Working Party, 'Opinion 4/2007' (n 86) 12-21.

Justice of the European Union ('CJEU') fully subscribes to the broad interpretation proposed by the Article 29 Working Party. Indeed, as Purtova remarkably explained, even though an IP address precisely aims at distinguishing someone, the CJEU held in the landmark *Breyer*[91] case that an IP address does not in itself suffice to identify someone.[92] The CJEU's reasoning in *Breyer* would support the interpretation of identification as knowing the identity of someone, a higher threshold than the one proposed by the Article 29 Working Party.[93] The recent *SRB*[94] case again focuses on the identifiability criterion, and much less on the identification aspect. It does not judge in favour of one or the other interpretation of identification, but again suggests a slight (but inconclusive) indication in favour of the identification as 'knowing the identity' interpretation. According to the CJEU, 'pseudonymisation (…) refers to the establishment of technical and organisational measures to reduce the risk of a data set being correlated with the *identity* of data subjects.'[95]

Aside from the fact that the identification requirement remains unclear today – which is as such a major issue for data protection law, as this concept is a determining factor of application of the GDPR, the available interpretations of the identification requirement are both unfit to appropriately protect data subjects. On the one hand, the identification as 'singling out' interpretation would lead to an extremely wide application of the GDPR[96], resulting in the 'law of everything' issues discussed hereabove. On the other hand, the 'knowing the identity' interpretation would be too narrow, leaving data processing activities where the identity of individuals remains unknown (such as the processing of emotions via facial detection technologies discussed above), unchecked by the GDPR.

Finally, through the definition of personal data and the requirement of identification – even in the broad sense of 'singling out', individuals categorised as part of a group or category (which Purtova names 'classification identification') are not as such protected by the GDPR.[97] *A fortiori*, groups as such are also not protected by the GDPR. This focus on the individual as the unit of protection by the GDPR reveals its fundamentally individualistic approach.[98] This approach is flawed on three levels.

First, from a techno-societal perspective, and as discussed above, the individualistic approach fails to consider the relational turn of data processing activities. Today, data processing activities are frequently based on clustering or group

[91] *Patrick Breyer v Bundesrepublik Deutschland*, Case C-582/14, [2016] ECLI:EU:C:2016:779.
[92] Purtova, 'From Knowing by Name to Targeting' (n 74) 178–180.
[93] ibid 166.
[94] *EDPS v SRB*, Case C-413/23, [2025] ECLI:EU:C:2025:645.
[95] *EDPS v SRB* (n 94) para 72 (emphasis added).
[96] Purtova, 'From Knowing by Name to Targeting' (n 74) 181.
[97] Purtova, 'From Knowing by Name to Targeting' (n 74).
[98] Luciano Floridi, 'Open Data, Data Protection, and Group Privacy' (2014) 27 Philosophy & Technology 1; Renieris (n 24) 70–73; Solow-Niederman (n 54).

classification as well as (resulting) inferences by association.[99] If we set the material scope of the GDPR aside, a good example is predictive policing, where historic crime data of a group (eg a neighbourhood) are used to allegedly predict and anticipate future crimes in the same group. Even though individuals would feel the effect of this data processing activity, individuals were not targeted as such, it is the group that is targeted.[100]

Second, as discussed above, individual rights providing control to data subjects do not scale. People are often unable to truly exercise their individual rights. These rights may thus not be acted upon and remain unenforced, which may harm society (see third flaw below).

Third, the individualistic approach fails to consider that individual rights also serve society at large. The Cambridge Analytica scandal is a good example of how the violation of individual rights to data protection can harm society and democracy.

# 4 Potential Solutions

## 4.1 Mainstream Approach: More or Enhanced Rights

In light of gaps in the data protection framework, the conventional doctrinal response consists in the creation of novel rights or in the enhancement of existing rights.[101] So, Farahany for instance argues in favour of a new right to cognitive liberty.[102] In their seminal article, Wachter and Mittelstadt propose a new 'right to reasonable inferences' consisting in two facets, one that would function *ex ante* (the notification obligation to the data subject), and another that would function *ex post* (the right for data subjects to object, with hope for a dialogue between the data subject and the controller).[103] Ienca and Andorno called for the creation of additional rights, such as the rights to cognitive liberty, mental privacy and psychological continuity.[104] Concluding that the existing human rights framework is inappropriate, Renieris also

[99] Purtova, 'From Knowing by Name to Targeting' (n 74) 182; Oskar J Gstrein and Anne Beaulieu, 'How to Protect Privacy in a Datafied Society? A Presentation of Multiple Legal and Conceptual Approaches' (2022) 35 Philosophy & Technology 3, 28.
[100] Gstrein and Beaulieu (n 99) 28.
[101] Lokke Moerel, 'Metaverse and Data Protection' in Larry A DiMatteo and Michel Cannarsa (eds), *Research Handbook on the Metaverse and Law* (Edward Elgar Publishing 2024) 129 <https://www.elgaronline.com/view/book/9781035324866/book-part-9781035324866-15.xml> accessed 30 October 2025.
[102] Farahany (n 35).
[103] Sandra Wachter and Brent Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' [2019] Columbia Business Law Review 494.
[104] Marcello Ienca and Roberto Andorno, 'Towards New Human Rights in the Age of Neuroscience and Neurotechnology' (2017) 13 Life Sciences, Society and Policy 5.

recommends the creation of new rights such as neuro-rights.[105] In its recent 'Recommendation on the Ethics of Neurotechnology', the mechanisms of consent and transparency represent pivotal tenets of the recommendation.[106]

These initiatives are laudable insofar as they are (explicitly[107] or tacitly) normatively based on the values of autonomy and self-determination. However, we suggest that it is these very praiseworthy values that are eventually harmed. Indeed, and as we have shown, autonomy can only be leveraged to a certain extent. Beyond that, it becomes an autonomy trap, as rights can at best be exercised within strict parameters that are rarely met. Such parameters have been well defined by Solove[108] as well as Solow-Niederman[109]. In short, and assuming that 'owners' of rights are rational agents (which is not a given[110]), owners of rights must be aware of the existence of their right, be informed that their right was or will be interfered with (which is a problem if privacy policies are too long or too complex for instance), have the resources (including in terms of time and money) to exercise their right and to understand the costs and benefits of (not) acting, and be free to exercise their right (which would for instance not be the case in situation of great power asymmetry, if manipulation, dark patterns or nudges are used, or if (not) exercising the right is a pre-condition to actively participate in society).

It is evident that, in the context of these stringent parameters, the exercise of rights is frequently compromised, resulting in adverse consequences for the owners of those rights, as well as for related individuals - as data protection has evolved from an individual concern to a collective responsibility.[111]

## 4.2 Proposed Approach

We have posited (see our section on '**Error! Reference source not found.**') that the GDPR is still based on the relationships and principles of the 70s and 80s. The scope of this article precludes a comprehensive revision of the GDPR that would better fit the world of today and tomorrow. This requires a thorough analysis from the EU lawmaker, together with key stakeholders to revise the data protection framework considering concrete facts and data.

[105] Renieris (n 24). Renieris does not only recommend the creation of new rights, she also argues in favour of the top-down approach that we discuss below.
[106] Unesco, 'Draft Recommendation on the Ethics of Neurotechnology' (*Unesco*, November 2025) <https://unesdoc.unesco.org/ark:/48223/pf0000394866> accessed 9 November 2025.
[107] ibid; Farahany (n 35) 186.
[108] Solove (n 55).
[109] Solow-Niederman (n 54).
[110] Richard H Thaler and Cass R Sunstein, *Nudge: Improving Decisions about Health, Wealth, and Happiness* (Yale University Press 2008).
[111] Solow-Niederman (n 54) 28–32.

Notwithstanding the foregoing, we can propose ways forward, which will then have to be complemented by further research. Below, we will suggest ways to address the following issues and gaps: the 'law of everything', the low protection of emotion and mental data, the lack of clarity of the identification requirement, as well as the individualistic nature of the GDPR.

### 4.2.1 Addressing the Law of Everything and Lack of Protection by Article 9

First, with regard to the 'law of everything' issue and the fact that the processing of emotion and mental data are not prohibited by Article 9 of the GDPR, we suggest a top-down approach from the EU lawmaker, that would forbid the processing of emotion and mental data for commercial purposes, and only allow such processing for limited purposes (such as health or research). Proxies of emotion and mental data (such as gaze) could be processed to the extent strictly necessary to provide the service, subject to the other principles of the GDPR (in particular data minimisation and storage retention), and without any allowed inference of emotion and mental data. As a result, the control would be exercised by the EU lawmaker, and no longer by data subjects, thereby scaling down the pressure on their autonomy and control. As Moerel nicely puts it '[p]rivacy legislation needs to regain its role of determining what is and is not permissible. Instead of a legal system based on user consent, we need to re-think the social contract for our digital society by discussing where the red lines for data use should be drawn.'[112] This top-down approach should not only be focussed on emotion and mental data, but apply more broadly throughout the GDPR, to release the pressure on the transparency and consent mechanisms and in turn, on data subjects.

One could counter-argue that such approach would be paternalistic, thereby reducing the autonomy of data subjects. This criticism would in our view only make sense in theory but be contradicted by the practical reality. Indeed, as we have shown above, there is sufficient research demonstrating that the current bottom-up model does not work in practice and exhausts the autonomy and control of data subjects. Sunstein explained that perfectly in his seminal work 'The Ethics of Influence':

> 'autonomy does not require choices everywhere; it does not justify an insistence on active choosing in all contexts. […] People should be allowed to devote their attention to the questions that, in their view, deserve attention. If people have to make choices everywhere, their autonomy is reduced, if only

[112] Moerel (n 101) 132.

> because they cannot focus on those activities that seem to them most worthy of their time.'[113]

Besides, as Dworkin explains, true paternalism requires 'that the person who is treated paternalistically does not wish to be treated that way' and would have decided otherwise in the absence of the paternalistic decision.[114] Research shows that, in the vast majority situations, even though people would have preferred to be protected by applicable privacy and data protection frameworks, in practice, they failed to protect themselves and consented to the data protection activity at hand. This is the so-called 'privacy paradox'.[115] Consequently, the act cannot be regarded as an instance of paternalism if the decision that is purportedly made in a paternalistic manner merely permits the decision that would have been taken by the data subject concerned, had the stringent parameters of control (outlined above) been adhered to. In such a case, it cannot be considered an interference with the autonomy of the data subjects; rather, it is a protection of that autonomy.

### 4.2.2 Addressing the Issues with the Identification Requirement

As explained above, next to the fact that it is unclear, the identification requirement is fraught with pitfalls. Thus, interpreted as 'singling out', it quickly leads to the 'law of everything' issue. Interpreted as knowing the identity, it is too restrictive and fails to protect data subjects. Besides, it reveals the individualistic approach of the GDPR, which fails to protect individuals as members of groups. Against that background, we propose the following adaptations to the GDPR, which should be further analysed to be implemented in the context of the Digital Omnibus reform. These suggestions try to stick as close as possible to the current wording and rationale of the GDPR.

First, regarding the 'law of everything' problem, every practitioner of the GDPR has already faced situations where the GDPR should in theory be fully respected, even though it would seem absurd in the circumstances at hand. For instance, in a B2B context, if two companies sign a contract, individuals would need to represent them. The mere mention of individuals representing the company, as well as their signature, would trigger the whole data protection framework. In our humble view, this is nonsense.

To substantially limit the 'law of everything' problem, we suggest to slightly complement the definition of 'processing' (Article 4(2) of the GDPR) with the wording from Article 22 of the GDPR, as indicated with the underlining:

[113] Sunstein (n 49) 65.
[114] Dworkin (n 35) 123.
[115] Daniel J Solove, *On Privacy and Technology* (Oxford University Press 2025) 20–21.

> 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, and which produces legal effects concerning the data subject or similarly significantly affects the data subject, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction which legally or significantly affects the data subject'.[116]

Reusing the wording of Article 22 has the merit of using concepts that were already deemed acceptable, and that have already been interpreted by case-law[117], authorities[118], and legal scholarship.[119]

As a result, the GDPR would only apply if a data processing activity concretely affects the data subject (factually and/or legally). If the data processing activity has no consequences for the data subject, or only trivial consequences, the GDPR would not apply. This approach is in line with the recommendation of certain authors to shift the locus of regulation from the technology to the concrete consequences thereof.[120]

Second, to address the 'law of nothing' problem (ie the fact that a person's personal data might be processed but not protected by the GDPR if the controller does not identify the person), we recommend abandoning the 'identification' requirement altogether. Indeed, this requirement is not necessary, notably as it is to a certain extent linked to the 'relate to' requirement[121], which we would suggest keeping.

Concretely, we would define personal data as 'any information relating to a natural person as individual or member of a group'. As a result, individuals would be protected by the GDPR if information about them is processed (the 'content' aspect

---

[116] Emphasis added.

[117] *Schufa Holding*, Case C-634/21, [2023] ECLI:EU:C:2023:957.

[118] See eg the guidelines of the former Article 29 Working Party. Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (WP 251, 6 February 2018).

[119] Lee A Bygrave, 'Article 22 Automated Individual Decision-Making, Including Profiling' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020).

[120] Solove for instance recommends to rather address uses, harms and risks. See Daniel J Solove, 'Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data' (2024) 118 Northwestern University Law Review. Purtova considers the idea of abandoning the concept of personal data and rather focus on 'information-induced harms'. See Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (n 39) 34. This is also one of the key arguments of Bennett Moses. See Lyria Bennett Moses, 'Regulating in the Face of Sociotechnical Change' in Roger Brownsword, Eloise Scotford and Karen Yeung (eds), *The Oxford Handbook of Law, Regulation and Technology* (Oxford University Press 2017) <https://doi.org/10.1093/oxfordhb/9780199680832.013.49> accessed 11 November 2025.

[121] Lorenzo Dalla Corte, 'Scoping Personal Data: Towards a Nuanced Interpretation of the Material Scope of EU Data Protecton Law' (2019) 10 European Journal of Law and Technology 9–10.

of the 'relating to' criterion), or if processed information influences (the 'purpose' aspect of the 'relating to' criterion) or impacts (the 'result' aspect of the 'relating to' criterion) a person, but only to the extent that the processing activity legally or significantly affects the data subject (see our proposed revised definition of 'processing').

This revised definition – encompassing individuals as members of a group - together with Article 80 of the GDPR (which allows associations to act in the name of individuals) would finally go in the direction of 'group privacy' and eventually protect individuals which are not targeted as isolated persons, but as members of a group.

## 5 Conclusion

This article has assessed whether the GDPR, presented as technologically neutral, will provide a robust framework for the metaverse. Our analysis has critically examined the GDPR as both the 'law of everything' and the 'law of nothing', revealing fundamental tensions in the European data protection framework when confronted with metaversal technologies.

The 'law of everything' problem stems from the metaverse's 'always-on recording' system, where sensors massively process real world data to influence the digital world, causing everything to become data. This leads to a system overload for the actors of the GDPR (controllers, processors, data subjects and data protection authorities), undermining meaningful compliance, whilst simultaneously overwhelming data subjects with rights that cannot be meaningfully exercised, transforming control into a mere illusion. These pitfalls expose the GDPR's obsolescence: whilst its core principles date back to the Fair Information Practices Principles of the 1970s and 1980s, designed for bi-directional state-citizen relationships, today's multi-directional data processing environment has evolved dramatically.

Conversely, the 'law of nothing' problem arises from the metaverse's immersive nature, which brings about the processing of emotions and mental data. However, emotion and mental data are not considered sensitive under Article 9 of the GDPR, despite being among the most intimate information about people. Moreover, the identification requirement under Article 4(1) of the GDPR remains unclear and unfit: interpreted as 'singling out', it leads to the 'law of everything' problem; interpreted as 'knowing the identity', it is too restrictive, leaving unchecked data processing activities where individuals' identities remain unknown. Furthermore, the GDPR's fundamentally individualistic approach fails to protect individuals as members of groups, ignoring the relational turn of data processing activities based on clustering

and group classification, and neglecting how violations of individual rights can harm society at large.

We have finally critically examined the mainstream doctrinal response of creating novel rights or enhancing existing rights, arguing that whilst laudable in their normative basis on autonomy and self-determination, these initiatives ultimately harm the very values they seek to protect, as rights can only be exercised within strict parameters that are rarely met, and data protection has evolved from an individual concern to a collective responsibility. Instead, we have proposed a top-down approach whereby the EU lawmaker would forbid the processing of emotion and mental data for commercial purposes, thereby scaling down the pressure on data subjects' autonomy and control. This approach is not paternalistic but rather protective of autonomy, as research demonstrates that the current bottom-up model exhausts data subjects' autonomy. To address the 'law of everything' problem, we have suggested complementing the definition of 'processing' to ensure the GDPR only applies when data processing activities concretely affect data subjects, thereby slightly shifting the locus of regulation from technology to concrete consequences. To address the 'law of nothing' problem, we have recommended abandoning the identification requirement and redefining personal data as 'any information relating to a natural person as individual or member of a group', thereby moving towards group privacy and protecting individuals targeted as members of groups.

The metaverse thus serves as a revealing lens through which the structural limitations of contemporary data protection law become visible. Our analysis demonstrates that the GDPR's foundational pillars, when confronted with metaversal technologies, risk collapsing under their own weight. It is striking that whilst the GDPR grounds itself in well defined core values, it has failed to afford heightened protection to the very data that constitute the closest substrate of these values. This paradox reveals a deeper tension: the GDPR's commitment to abstract values applied theoretically has obscured the need for concrete, sociotechnical-sensitive safeguards that actually preserve these values and respond to the material realities of contemporary data processing.

## Bibliography

## Primary sources

Article 29 Working Party. Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (WP 251, 6 February 2018)

Charter of Fundamental Rights of the European Union, OJ 2010 C 83/389

Commission, 'Commission Staff Working Document Accompanying the document: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions : An EU initiative on Web 4.0 and virtual worlds : a head start in the next technological transition' SWD(2023) 250 final

— —, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions : An EU initiative on Web 4.0 and virtual worlds: a head start in the next technological Transition' (Communication) COM(2023) 442 final

— —, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions : Long-term competitiveness of the EU: looking beyond 2030' (Communication) COM(2023) 168 final

— — ,'Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2016/1036, (EU) 2016/1037, (EU) 2017/1129, (EU) 2023/1542 and (EU) 2024/573 as regards the extension of certain mitigating measures available for small and medium sized enterprises to small mid-cap enterprises and further simplification measures' COM(2025) 501 final/2 (GDPR Omnibus)

Consolidated Version of the Treaty on the Functioning of the European Union [2016] OJ C 202/1

Council of the European Union, 'Metaverse: Virtual World, Real Challenges' (2023) <https://data.europa.eu/doi/10.2860/432862> accessed 13 January 2023

EDPS v SRB, Case C-413/23, [2025] ECLI:EU:C:2025:645

Garante per la protezione dei dati personali (9896808, 2023) < https://garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9896808> accessed 18 August 2023

Patrick Breyer v Bundesrepublik Deutschland, Case C-582/14, [2016] ECLI:EU:C:2016:779

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) [2016], OJ L119/1

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) [2022] OJ L265/1

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) [2022], OJ L277/1

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) [2024], OJ L

Schufa Holding, Case C-634/21, [2023] ECLI:EU:C:2023:957

Unesco, 'Draft Recommendation on the Ethics of Neurotechnology' (Unesco, November 2025) <https://unesdoc.unesco.org/ark:/48223/pf0000394866> accessed 9 November 2025

## Secondary Sources

Accenture, 'The Post-Digital Era is Upon Us : Are You Ready For What's Next?' (2019) <https://www.accenture.com/content/dam/accenture/final/a-com-migration/r3-additional-pages-1/pdf/pdf-94/accenture-techvision-2019-exec-summary.pdf> accessed 12 November 2025

Aimen T, 'Cognitive Freedom and Legal Accountability: Rethinking the EU AI Act's Theoretical Approach to Manipulative AI as Unacceptable Risk' (2025) 1 Cambridge Forum on AI: Law and Governance e20

Ball M, The Metaverse: And How It Will Revolutionize Everything (Liveright 2022)

Basdevant A, François C and Ronfard, 'Mission exploratoire sur les métavers' (October 2022) 35 <https://www.economie.gouv.fr/files/files/2022/Rapport-interministeriel-metavers.pdf> accessed 7 June 2023

Bennett Moses L, 'Regulating in the Face of Sociotechnical Change' in Roger Brownsword, Eloise Scotford and Karen Yeung (eds), The Oxford Handbook of Law, Regulation and Technology (Oxford University Press 2017) <https://doi.org/10.1093/oxfordhb/9780199680832.013.49> accessed 11 November 2025

Brave, 'Europe's governments are failing the GDPR. Brave's 2020 report on the enforcement capacity of data protection authorities' (2020) <https://brave.com/blog/dpa-report-2020/> accessed 30 October 2025

Bygrave LA, Data Protection Law: Approaching Its Rationale, Logic and Limits (Wolters Kluwer Law International 2002)

— —, 'Article 22 Automated Individual Decision-Making, Including Profiling' in Christopher Kuner and others (eds), The EU General Data Protection Regulation (GDPR): A Commentary (Oxford University Press 2020)

Calo R and others, 'Augmented Reality: A Technology and Policy Primer' [2016] Tech Policy Lab <https://digitalcommons.law.uw.edu/techlab/1>

Clifford D, Data Protection Law and Emotion (1st edn, Oxford University Press 2024)

Dalla Corte L, 'Scoping Personal Data: Towards a Nuanced Interpretation of the Material Scope of EU Data Protecton Law' (2019) 10 European Journal of Law and Technology

De Hert P and Gutwirth S, 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action' in Serge Gutwirth and others (eds), Reinventing Data Protection? (Springer 2009)

Dèbes F, 'Mark Zuckerberg, l'aventurier tenace du métavers et des mondes virtuels' (Les Echos, 28 September 2024) <https://www.lesechos.fr/tech-medias/hightech/mark-zuckerberg-laventurier-tenace-du-metavers-et-des-mondes-virtuels-2121928> accessed 24 October 2025

DeNardis L, The Internet in Everything: Freedom and Security in a World with No Off Switch (Yale University Press 2020)

Düwell M, 'Human Dignity and the Ethics and Regulation of Technology' in Roger Brownsword, Eloise Scotford and Karen Yeung (eds), The Oxford Handbook of Law, Regulation and Technology, vol 1 (Oxford University Press 2017)

Dworkin G, The Theory and Practice of Autonomy (Cambridge University Press 1988)

Egliston B and Carter M, 'Critical Questions for Facebook's Virtual Reality: Data, Power and the Metaverse' (2021) 10 Internet Policy Review <https://policyreview.info/articles/analysis/critical-questions-facebooks-virtual-reality-data-power-and-metaverse> accessed 28 October 2025

Farahany NA, The Battle for Your Brain: Defending the Right to Think Freely in the Age of Neurotechnology (First edition, St Martin's Press 2023)

Fia T, 'Fairness in Market Instrumental Data Law' (2025) 33 International Journal of Law and Information Technology

Floridi L, 'Open Data, Data Protection, and Group Privacy' (2014) 27 Philosophy & Technology 1

Friedl P, Reasonable Expectations of Privacy: With Special Regard to European Privacy and Data Protection Law (1st ed. 2025, Springer Nature Switzerland 2025)

Georgieva L and Kuner C, 'Article 9 Processing of Special Categories of Personal Data' in Christopher Kuner and others (eds), The EU General Data Protection Regulation (GDPR) (Oxford University Press 2020)

Goulard H, 'Le métavers à la relance' (Les Echos, 6 February 2024) <https://www.lesechos.fr/idees-debats/editos-analyses/le-metavers-a-la-relance-2074303> accessed 24 October 2025

Gstrein OJ and Beaulieu A, 'How to Protect Privacy in a Datafied Society? A Presentation of Multiple Legal and Conceptual Approaches' (2022) 35 Philosophy & Technology

Hartzog W, Privacy's Blueprint: The Battle to Control the Design of New Technologies (Harvard University Press 2018)

Häuselmann A, 'Fit for Purpose? Affective Computing Meets EU Data Protection Law' (2021) 11 International Data Privacy Law 245

Ienca M and Andorno R, 'Towards New Human Rights in the Age of Neuroscience and Neurotechnology' (2017) 13 Life Sciences, Society and Policy

Ienca M and Malgieri G, 'Mental Data Protection and the GDPR' (2022) 9 Journal of Law and the Biosciences

Kuner C, 'The Draghi Dilemma: The Right and the Wrong Way to Undertake GDPR Reform' (Future of Privacy Forum, 23 October 2025) <https://fpf.org/blog/the-draghi-dilemma-the-right-and-the-wrong-way-to-undertake-gdpr-reform/> accessed 27 October 2025

Maciejewski M, 'Metaverse' (European Parliament, 2023) < https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2023)751222 > accessed on 20 October 2023

Madiega T, Car P and Niestadt M, 'Metaverse: Opportunities, risks and policy implications'( European Parliament, 2022) <https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733557> accessed 13 January 2023

McDonald AM and Cranor LF, 'The Cost of Reading Privacy Policies'(2008) 4 A Journal of Law and Policy for the Information Society 543

McGill M, 'The IEEE Global Initiative on Ethics of Extended Reality (XR) Report–Extended Reality (XR) and the Erosion of Anonymity and Privacy' (IEEE, November 2021) <https://ieeexplore.ieee.org/document/9619999> accessed 28 October 2025

McStay A, 'Emotional AI, Soft Biometrics and the Surveillance of Emotional Life: An Unusual Consensus on Privacy' (2020) 7 Big Data & Society

Meta, 'Introduction Meta : A Social Technology Company' <https://about.fb.com/news/2021/10/facebook-company-is-now-meta/> accessed 24 October 2024

Moerel L, 'Metaverse and Data Protection' in Larry A DiMatteo and Michel Cannarsa (eds), Research Handbook on the Metaverse and Law (Edward Elgar Publishing 2024) <https://www.elgaronline.com/view/book/9781035324866/book-part-9781035324866-15.xml> accessed 30 October 2025

Purtova N, 'Default Entitlements in Personal Data in the Proposed Regulation: Informational Self-Determination off the Table … and Back on Again?' (2014) 30 Computer law & security review 6

— —, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10 Law, Innovation and Technology 40

— —, 'From Knowing by Name to Targeting: The Meaning of Identification under the GDPR' (2022) 12 International Data Privacy Law 163

Renieris EM, Beyond Data: Reclaiming Human Rights at the Dawn of the Metaverse (The MIT Press 2023)

Richards N and Hartzog W, 'Taking Trust Seriously in Privacy Law' (2016) 19 Stanford Technology Law Review 431

— —, 'The Pathologies of Digital Consent' (2019) 96 Washington University Law Review 1461

Rose S, '"The Metaverse Will Be Our Slow Death!" Is Facebook Losing Its $100bn Gamble on Virtual Reality?' The Guardian (7 December 2022) <https://www.theguardian.com/technology/2022/dec/07/metaverse-slow-death-facebook-losing-100bn-gamble-virtual-reality-mark-zuckerberg> accessed 24 October 2025

Schwab P-N, 'Reading Privacy Policies of the 20 Most-Used Mobile Apps Takes 6h40' (Into the Minds, 28 May 2018) <https://www.intotheminds.com/blog/en/reading-privacy-policies-of-the-20-most-used-mobile-apps-takes-6h40/> accessed 30 October 2025

Solove DJ, 'Introduction: Privacy Self-Management and the Consent Dilemma' (2013) 126 Harvard law review 1880

— —, 'Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data' (2024) 118 Northwestern University Law Review

— —, On Privacy and Technology (Oxford University Press 2025)

Solow-Niederman A, 'Information Privacy and the Inference Economy' (2022) 117 Northwestern University Law Review 357

Stephenson N, Snow Crash (Bantam 1992)

Sunstein CR, The Ethics of Influence: Government in the Age of Behavioral Science (Cambridge University Press 2016) <https://www.cambridge.org/core/books/ethics-of-influence/E29EDE19EBCB53F6D8691730668115F7> accessed 30 October 2025

Susskind J, The Digital Republic: Taking Back Control of Technology (Bloomsbury Publishing 2023)

Thaler RH and Sunstein CR, Nudge: Improving Decisions about Health, Wealth, and Happiness (Yale University Press 2008)

Timan T, Galič M and Koops B-J, 'Surveillance Theory and Its Implications for Law' in Roger Brownsword, Eloise Scotford and Karen Yeung (eds), The Oxford Handbook of Law, Regulation and Technology (Oxford University Press 2017)

Wachter S and Mittelstadt B, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' [2019] Columbia Business Law Review 494

Xynogalas V and Leiser M, 'The Metaverse: Searching for Compliance with the General Data Protection Regulation' (2024) 14 International Data Privacy Law 89

## Short bio

***Cyril Fischer*** obtained a Master of Laws at University of Liège, followed by an LLM from the LSE in 2018. Since June 2022, he has been a PhD candidate at the University of Liège, where he also lectures on Data Protection Law. His publications include *Gouvernance par le consentement, big data et nouveau droit européen des données: dans quelle mesure le Data Act et le Data Governance Act favorisent-ils le big data?* and *Re-thinking the allocation of roles under the GDPR in the context of cloud computing* (International Data Privacy Law, OUP). He is also a guest lecturer at HEC and teaches the course AI & Metaverse at the Brussels School of Competition. Since 2018, he has been a Senior Associate Lawyer at Stibbe.