ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών

«ΔΙΚΑΙΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ»

Ακαδημαϊκό έτος 2021-2022

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της Γεωργίας Πατήρη (Α.Μ.: 2139)

METAVERSE ΚΑΙ ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ: ΣΥΜΒΑΤΟΤΗΤΑ ΚΑΙ ΝΟΜΙΚΕΣ ΠΡΟΚΛΗΣΕΙΣ ΥΠΟ ΤΟ ΦΩΣ ΤΟΥ ΓΚΠΔ

Επιβλέπουσα:

Δρ. Μαρίνα Μαρκέλλου

Πειραιάς, Ιούνιος 2023

Στον παππού μου, Γιάννη.

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΛΗΨΗ 5

ABSTRACT 6

I. ΕΙΣΑΓΩΓΗ 7

II. ΚΥΡΙΩΣ ΜΕΡΟΣ

Α. ΕΞΕΡΕΥΝΩΝΤΑΣ ΤΟ METAVERSE 10

1. ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΙΔΕΑ ΤΟΥ METAVERSE 10

2. Η ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΤΟΥ METAVERSE 14

2.1 Κύρια χαρακτηριστικά 14

2.2 Τεχνολογίες αιχμής 18

2.3 Ανταγωνιστικά οράματα 28

3. ΤΟ METAVERSE ΩΣ ΝΕΑ ΕΠΕΝΔΥΤΙΚΗ ΤΑΣΗ 32

4. Η ΕΥΡΩΠΑΙΚΗ ΑΝΤΖΕΝΤΑ ΓΙΑ ΤΟ METAVERSE 37

Β. ΣΚΙΑΓΡΑΦΩΝΤΑΣ ΤΙΣ ΝΟΜΙΚΕΣ ΠΡΟΚΛΗΣΕΙΣ ΤΟΥ METAVERSE ΥΠΟ ΤΟ ΦΩΣ ΤΟΥ ΓΚΠΔ 42

1. Η ΓΕΝΕΣΗ ΤΟΥ ΔΙΚΑΙΩΜΑΤΟΣ ΣΤΑ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ ΚΑΙ Η ΘΕΣΠΙΣΗ ΤΟΥ ΓΚΠΔ 42

2. Η ΕΦΑΡΜΟΓΗ ΤΟΥ ΓΚΠΔ ΣΤΟ METAVERSE 43

2.1. Ουσιαστικό πεδίο εφαρμογής 43

2.2. Εδαφικό πεδίο εφαρμογής 49

3. ΕΙΔΙΚΑ ΖΗΤΗΜΑΤΑ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΟ METAVERSE 53

3.1. Επεξεργασία προσωπικών δεδομένων εξαγόμενων από συσκευές XR και παρεμφερείς τεχνολογίες 53

3.2. Κατανομή ρόλων μεταξύ των συμμετεχόντων μερών 63

3.3. Ενημέρωση των υποκειμένων και νόμιμες βάσεις επεξεργασίας 69

3.3.1. Η απαίτηση διαφάνειας της επεξεργασίας 70

3.3.2. Συναίνεση και άλλες νόμιμες βάσεις επεξεργασίας 72

3.4. Συμπεριφορική διαφήμιση και αλγοριθμική λήψη αποφάσεων 81

3.5. Διαβιβάσεις προσωπικών δεδομένων 90

3.5.1. Φορητότητα προσωπικών δεδομένων και διαλειτουργικότητα 90

3.5.2. Διαβίβαση προσωπικών δεδομένων εκτός ΕΕ 93
3.6. Ασφάλεια προσωπικών δεδομένων 95
3.7. Η (ασύμβατη;) σχέση μεταξύ ΓΚΠΔ και Blockchain 101
III. ΣΥΜΠΕΡΑΣΜΑΤΑ 104
IV. ΕΠΙΛΟΓΟΣ 109
V. ΒΙΒΛΙΟΓΡΑΦΙΑ 110

ΠΕΡΙΛΗΨΗ

Η παρούσα μεταπτυχιακή διπλωματική εργασία επικεντρώνεται στο ζήτημα της συμβατότητας και εν γένει των νομικών προκλήσεων που θα εγείρει το Metaverse σε σχέση με το ενωσιακό δίκαιο προστασίας προσωπικών δεδομένων και ειδικότερα, τον ΓΚΠΔ.

Η σχετική ανάλυση παρατίθεται σε δύο κεφάλαια. Στο Α' κεφάλαιο γίνεται μια εισαγωγή στην έννοια του Metaverse, αναλύονται τα βασικά χαρακτηριστικά του και οι επιμέρους τεχνολογίες που θα επιτρέψουν την υλοποίηση και την ουσιαστική λειτουργία του, αλλά και τα ανταγωνιστικά οράματα που έχουν επικρατήσει ως προς τη δομή και το μοντέλο διακυβέρνησής του. Επιπλέον, γίνεται μνεία στο ετερόκλητο επενδυτικό κοινό που έχει συγκεντρώσει και δίνεται έμφαση στους κυρίαρχους τομείς που αναμένεται αυτό να ενισχύσει και αναδιαμορφώσει. Το κεφάλαιο κλείνει με την περιγραφή της ατζέντας της ΕΕ για το Metaverse και τους λόγους για τους οποίους η παρούσα εργασία εστιάζει στη σχέση των ιδιωτικών πλατφορμών αυτού με το ενωσιακό δίκαιο προστασίας προσωπικών δεδομένων, δίνοντας έτσι τη σκυτάλη στο Β' κεφάλαιο.

Μια σύντομη αναφορά στη θεμελίωση του δικαιώματος στα προσωπικά δεδομένα και την πρόσφατη θέσπιση του ΓΚΠΔ από την ΕΕ, υπό το φως των νέων τεχνολογικών εξελίξεων, εγκαινιάζει το Β' κεφάλαιο. Ακολουθεί η διερεύνηση της ουσιαστικής και εδαφικής εφαρμογής του ΓΚΠΔ στο Metaverse. Περαιτέρω, εξετάζονται ενδελεχώς τα κύρια ζητήματα προστασίας προσωπικών δεδομένων που θα ανακύψουν λόγω της επικράτησης του τελευταίου στην ενωσιακή αγορά και προτείνονται λύσεις για το μετριασμό τους. Στο επίκεντρο των νομικών προκλήσεων τοποθετείται, μεταξύ άλλων, η μαζική επεξεργασία βιομετρικών και λοιπών προσωπικών δεδομένων που θα αντλούνται από τις ειδικές συσκευές εμβύθισης στο Metaverse, η δυσχέρεια σαφούς καθορισμού των υπόχρεων μερών, διαφανούς ενημέρωσης, λήψης της συναίνεσης των χρηστών και εξασφάλισης της νομιμότητας της επεξεργασίας των δεδομένων τους υπό το ισχύον νομοθετικό καθεστώς, οι ολέθριες συνέπειες της συμπεριφορικής διαφήμισης και της αλγοριθμικής λήψης αποφάσεων στη δυστοπική εκδοχή του Metaverse, η ανάγκη διασφάλισης της φορητότητας και της συνεχούς διαβίβασης προσωπικών δεδομένων εκτός ΕΕ για τη διαλειτουργικότητα του εικονικού κόσμου, η διακύβευση της ασφάλειας αυτών από εσωτερικές και εξωτερικές απειλές και τέλος, η αντίρροπη σχέση μεταξύ ΓΚΠΔ και Blockchain, ως τεχνολογίας στην οποία θα στηριχθεί, λιγότερο ή περισσότερο, η λειτουργία του Metaverse.

ABSTRACT

The present master's thesis focuses on the issue of compatibility and, in general, the legal challenges that the Metaverse will raise in relation to EU data protection law, specifically the GDPR.

The relevant analysis is presented in two chapters. Chapter A provides an introduction to the concept of the Metaverse, analyzes its basic characteristics, the specific technologies that will enable its implementation and effective functioning, as well as the competing visions that have prevailed regarding its structure and governance model. Additionally, reference is made to the diverse investment community it has attracted and emphasis is placed on the dominant sectors that are expected to be strengthened and reshaped by it. The chapter concludes with a description of the EU's agenda for the Metaverse and the reasons why this thesis focuses on the relationship of its private platforms with EU data protection law, thus setting the stage for Chapter B.

Chapter B begins with a concise reference to the foundation of the right to personal data and the recent establishment of the GDPR by the EU, in the light of new technological advancements. It then explores the substantive and territorial application of the GDPR in the Metaverse. Furthermore, it thoroughly examines the main data protection issues that will arise due to the latter's prevalence in the EU market and proposes solutions for their mitigation. Among the legal challenges, particular emphasis is laid upon the mass processing of biometric and other personal data extracted by specialized immersive devices in the Metaverse, the difficulty of clearly identifying the liable parties, ensuring transparent information, obtaining user consent and guaranteeing the lawfulness of the processing of their data under the current legislative framework, the detrimental consequences of behavioral advertising and algorithmic decision-making in the dystopian version of the Metaverse, the need to ensure portability and continuous transfer of personal data outside the EU for the interoperability of the virtual world, the jeopardization of their security by internal and external threats, and finally, the intricate relationship between the GDPR and Blockchain as the technology on which the operation of the Metaverse will rely, to a greater or lesser extent.

ΕΙΣΑΓΩΓΗ

Από την εμφάνισή του στη Γη, ο άνθρωπος πασχίζει να βελτιώσει τους όρους διαβίωσής του, οραματιζόμενος τρόπους να αποτιναχθεί από τα δεσμά της πεπερασμένης υλικής και πνευματικής του υπόστασης και να συνδεθεί οργανωτικά και συναισθηματικά με τους όμοιούς του.

Στο πλαίσιο αυτό, η ιδέα για μία δεύτερη ζωή διαποτίζει πλήθος εκδηλώσεων της ανθρώπινης δραστηριότητας· από τη λαϊκή παράδοση, τη θρησκεία και τις τέχνες μέχρι πρόσφατα, την τεχνολογία.

Βγαλμένη από σελίδες και σκηνές έργων επιστημονικής φαντασίας, η σύλληψη της ρεαλιστικής εμβύθισης του ανθρώπου στο *Metaverse*, έναν εικονικό, τρισδιάστατο και διαμοιραζόμενο κόσμο, εντός του οποίου βιώνει μια παράλληλη, τεχνητή πραγματικότητα, έχει πλέον μετουσιωθεί σε κυρίαρχο στόχο πολλών τεχνολογικών και λοιπών ιδιωτικών εταιρειών, υπόσχεται δε, όχι μόνο να αναδιαμορφώσει τα μέσα με τα οποία ο τελικός χρήστης καταναλώνει ψηφιακό περιεχόμενο, αγαθά και υπηρεσίες, αλλά εν γένει τον τρόπο με τον οποίο ο άνθρωπος κοινωνικοποιείται, εργάζεται, ψυχαγωγείται, διασκεδάζει, εκπαιδεύεται και τελικά ζει.

Οι τεχνολογικές και κοινωνιολογικές εξελίξεις των τελευταίων ετών ωθούν προς την κατεύθυνση του Metaverse, ως νέου σταθμού στην εξέλιξη του Διαδικτύου. Πράγματι, η ευρεία ψηφιοποίηση της κοινωνίας λόγω της πανδημίας COVID-19[1], η σταδιακή μετάβαση από συγκεντρωτικές (WEB 2.0) σε αποκεντρωμένες (WEB 3.0) διαδικτυακές εφαρμογές και εργαλεία[2], οι ραγδαίως αναπτυσσόμενες τεχνολογικές δυνατότητες[3], αλλά και οι μαζικές επενδύσεις στον τομέα από παράγοντες-κλειδιά[4], προμηνύουν πως το Metaverse ενδέχεται να γίνει "mainstream" πολύ πιο σύντομα από ότι αναμένεται.

---

[1] Ενδεικτικά, το 50% των Ευρωπαίων έχει στραφεί σε τουλάχιστον μερική τηλεργασία, συγκριτικά με το 12% πριν το ξέσπασμα της πανδημίας (βλ. Sandeepa, C., Wang, S. and Liyanage M. (2023) 'Privacy of the Metaverse: Current Issues, AI Attacks, and Possible Solutions', *IEEE International Conference on Metaverse Computing, Networking and Applications (IEEE MetaCom 2023)*, Κιότο, Ιαπωνία, 26-28 Ιουνίου 2023. ResearchGate (προδημοσίευση). Διαθέσιμο στο: https://www.researchgate.net/publication/369331696_Privacy_of_the_Metaverse_Current_Issues_AI_Attacks_and_Possible_Solutions, σ. 1).

[2] Βλ. Blockchain, κρυπτονομίσματα, NFTs κ.ά.

[3] Βλ. ChatGPT και DALL-E της OpenAI, 5G κ.ά.

[4] Βλ. επένδυση Meta Platforms στο Metaverse ύψους 10 δισεκατομμυρίων για το 2021, εξαγορά Activision Blizzard από τη Microsoft ύψους 69 δισεκατομμυρίων το 2022 κ.ά.

Παρά τα αδιαμφισβήτητα οφέλη που *υπόσχεται* να προσφέρει στο άτομο, την κοινωνία, την οικονομία, την επιστήμη, ακόμη και το περιβάλλον, βρίθουν οι φωνές που προειδοποιούν για τους πρωτοφανείς κινδύνους που ελλοχεύει για την ιδιωτικότητα των χρηστών του. Η ίδια η φύση του Metaverse, καθώς και οι επιμέρους τεχνολογίες που πρόκειται να υποστηρίξουν και να συνθέσουν το εικονικό σύμπαν, υπαγορεύει και θα επιτρέπουν, αντίστοιχα, την άνευ προηγουμένου συλλογή, αποθήκευση, διαβίβαση και εν γένει επεξεργασία των προσωπικών δεδομένων του χρήστη, ιδίως δε, ευαίσθητων πληροφοριών του τελευταίου που θα μπορούν να αποκαλύψουν, για πρώτη φορά στην ιστορία της ψηφιακής επανάστασης, τις πιο μύχιες πτυχές του εαυτού του. Το ανησυχητικό είναι ότι η εν λόγω επεξεργασία θα παρουσιάζεται ως απαραίτητη προϋπόθεση για τη λειτουργία του Metaverse, αλλά τελικά θα καταλήγει σε κατάρτιση διεισδυτικών προφίλ χρήστη για την εξυπηρέτηση ίδιων συμφερόντων των εμπλεκόμενων φορέων, ασύμβατων προς τους αρχικούς σκοπούς της επεξεργασίας. Η δυσχέρεια σαφούς καθορισμού των υπόχρεων μερών θα εντείνει την ανασφάλεια και την έκθεση σε κίνδυνο των υποκειμένων, οδηγώντας τους αρμόδιους σε αποποίηση ευθυνών και κατ' επέκταση παράλειψη νόμιμων υποχρεώσεων. Ελλείψει όμως ισχυρών προστατευτικών δικλείδων, το Metaverse θα αποτελέσει ένα χώρο ή καλύτερα, μια εποχή εκτεταμένων παραβιάσεων της ασφάλειας των προσωπικών δεδομένων των χρηστών του, τόσο από επιχειρηματικούς χρήστες, όσο και από κυβερνοεγκληματίες που θα σπεύσουν να εκμεταλλευτούν προς όφελός τους τις όποιες ευπάθειες του συστήματος.

Εκκινώντας από την αδιαπραγμάτευτη θέση ότι το Metaverse χρήζει νομοθετικής ρυθμίσεως, η παρούσα διπλωματική εργασία στοχεύει να διερευνήσει τη συμβατότητα και γενικότερα τις νομικές προκλήσεις του, υπό το φως του γενικού και οριζόντιου δικαίου προστασίας προσωπικών δεδομένων της ΕΕ, του ΓΚΠΔ· επίσης, να προτείνει ενδεικτικά ορισμένες λύσεις, με γνώμονα την αναγκαία εξισορρόπηση μεταξύ τεχνολογικής καινοτομίας, ελευθερίας της έκφρασης και πρόσβασης στην πληροφορία, αλλά και προστασίας της ιδιωτικότητας των χρηστών του.

Οπωσδήποτε, το σενάριο αποκλεισμού της ΕΕ από το Metaverse προδιαγράφει την τεχνολογική, οικονομική και πολιτική αποδυνάμωση της ΕΕ στο παγκόσμιο γίγνεσθαι, θυμίζει δε, συνθήκες απολυταρχικών καθεστώτων που αποσκοπούν στον αποκλεισμό των πολιτών τους από την ελεύθερη ενημέρωση. Αντίθετα, η έλλειψη αποτελεσματικών νομοθετικών και λοιπών ρυθμιστικών εργαλείων για τη διασφάλιση της προστασίας της

ιδιωτικότητας των υποκειμένων στο Metaverse, θα υλοποιήσει δυστοπικές ιστορίες γραμμένες χρόνια πριν, όπως το “The Truman Show” του Andrew Niccol και το “1984” του George Orwell.

I. ΚΥΡΙΩΣ ΜΕΡΟΣ

Α. ΕΞΕΡΕΥΝΩΝΤΑΣ ΤΟ METAVERSE

1. ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΙΔΕΑ ΤΟΥ METAVERSE

"The Metaverse is a massively scaled and interoperable network of real-time rendered 3D virtual worlds and environments which 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."[5]

Η ιδέα για το Metaverse δεν αποτελεί κατάκτηση του 21ου αιώνα· ψήγματά της εντοπίζονται σε διάφορες κουλτούρες και εποχές, διατρέχοντας μέχρι και τα αρχαία χρόνια και την Αλληγορία του Σπηλαίου του Πλάτωνα[6]. Επισήμως, ο όρος "Metaverse" γεννάται το 1992 από τον Αμερικανό συγγραφέα επιστημονικής φαντασίας Neal Stephenson[7]. Στο κυβερνοπάνκ μυθιστόρημά του με τίτλο "Snow Crash", ο Stephenson οραματίζεται μια δυστοπική αμερικανική κοινωνία από την οποία ο Hiro Protagonist, κεντρικός ήρωας του βιβλίου, δραπετεύει μέσω ενός εικονικού κόσμου, του Metaverse[8] [9]. Το 2003, κυκλοφορεί η πλατφόρμα Second Life της Linden Lab, εντός της οποίας οι χρήστες κοινωνικοποιούνται

---

[5] Ball, M. (2021) 'Framework for the Metaverse — MatthewBall.vc', *MatthewBall.vc*, 29 Ιουνίου. Διαθέσιμο στο: https://www.matthewball.vc/all/forwardtothemetaverseprimer [Πρόσβαση 5 Μαΐου 2023].

[6] Di Pietro, R. and Cresci, S. (2021) 'Metaverse: Security and Privacy Issues', *2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, Ατλάντα, Τζόρτζια, ΗΠΑ, 13-15 Δεκεμβρίου. IEEE, σ. 281-288. Διαθέσιμο στο: https://doi.org/10.1109/tpsisa52974.2021.00032, σ. 281.

[7] Aamir, O. (2022) 'Metaverse and its regulation', *SSRN Electronic Journal*, 29 Δεκεμβρίου. Διαθέσιμο στο: https://doi.org/10.2139/ssrn.4306357, σ. 7.

[8] Wikipedia (2023*) Snow Crash*. Διαθέσιμο στο: https://en.wikipedia.org/wiki/Snow_Crash [Πρόσβαση 5 Μαΐου 2023].

[9] Αντίστοιχα, στην κινηματογραφική μεταφορά του μυθιστορήματος επιστημονικής φαντασίας του Ernest Cline με τίτλο "Ready Player One" από τον Steven Spielberg το 2018, οι άνθρωποι εν έτει 2045 εγκαταλείπουν τον πραγματικό κόσμο μέσω ενός εικονικού σύμπαντος, ονόματι "The Oasis"(βλ. Tucci, L. (2023) 'What is the metaverse? An explanation and in-depth guide', *WhatIs.com*, 25 Απριλίου. Διαθέσιμο στο: https://www.techtarget.com/whatis/feature/The-metaverse-explained-Everything-you-need-to-know [Πρόσβαση 5 Μαΐου 2023]), ενώ το 2019, το επεισόδιο Striking Vipers της τηλεοπτικής σειράς Black Mirror αποτύπωσε με τον πιο αληθοφανή τρόπο το πώς θα μοιάζει το Metaverse στο εγγύς ή απώτερο μέλλον.

χωρίς καθορισμένο στόχο, ζώντας μια δεύτερη, παράλληλη εικονική ζωή ως άβαταρ[10]. Το Second Life και τα διαδικτυακά παιχνίδια ρόλων πολλαπλών παικτών, κοινώς γνωστά ως "MMORPGs"[11], θεωρούνται οι προπομποί του (proto-Metaverses)[12].

Η αναζωπύρωση της συζήτησης γύρω από το Metaverse και τις συναρπαστικές δυνατότητές του χρονολογείται μόλις τον Οκτώβριο του 2021, όταν ο Mark Zuckerberg[13] ανακοινώνει πανηγυρικά την αλλαγή της επωνυμίας του ομίλου Facebook Inc. σε Meta Platforms Inc.[14], εγκαινιάζοντας έτσι το όραμά του για το Metaverse[15]. Έκτοτε, το επενδυτικό ενδιαφέρον εκτοξεύεται κατακόρυφα, όχι μόνο στους κόλπους της Silicon Valley, αλλά και πολλών κέντρων καινοτομίας ανά τον πλανήτη. Ήδη κορυφαίες εταιρείες τεχνολογίας, παγκοσμίου φήμης εμπορικά σήματα (brands) και λοιπά ενδιαφερόμενα μέρη επισπεύδουν μαζικά τις ενέργειές τους για την είσοδο και δραστηριοποίησή τους στον εν λόγω χώρο.

Τι είναι, λοιπόν, στην πραγματικότητα το Metaverse;

Ο όρος "Metaverse" συντίθεται από την ελληνική λέξη «μετά» και την αγγλική λέξη "universe", που μεταφράζεται ως «σύμπαν»[16]. Στην ελληνική γλώσσα, αποδίδεται ως «Μετασύμπαν». Η προσπάθεια να οριστεί η *φύση* του Metaverse μοιάζει εν πολλοίς με την απόπειρα να περιγραφεί η πορεία του Internet το 1990 ή να προβλεφθεί η επανάσταση που θα επέφερε η επικράτηση των έξυπνων τηλεφώνων (smartphones) στην καθημερινή ζωή το

---

[10] Επίσης, οι χρήστες μπορούν να δημιουργούν, να αγοράζουν και να πωλούν ψηφιακά περιουσιακά στοιχεία μέσω του εικονικού νομίσματος Linden (βλ. Βικιπαίδεια (2023) *Second Life*. Διαθέσιμο στο: https://el.wikipedia.org/wiki/Second_Life [Πρόσβαση 5 Μαΐου 2023]).

[11] Massively multiplayer online role-playing games, όπως το World of Warcraft (WoW) της Blizzard Entertainment, το Star Wars: The Old Republic της BioWare κ.ο.κ.

[12] Citi GPS: Global Perspectives & Solutions (2022) 'Metaverse and Money Decrypting the Future'. Διαθέσιμο στο: https://ir.citi.com/gps/x5%2BFQJT3BoHXVu9MsqVRoMdiws3RhL4yhF6Fr8us8oHaOe1W9smOy1%2B8aaAgT3SPuQVtwC5B2%2Fc%3D, σ. 14.

[13] Ιδρυτής, πλειοψηφών μέτοχος και Διευθύνων Σύμβουλος (CEO) του ομίλου εταιρειών με την (τέως) επωνυμία Facebook Inc., ο οποίος ελέγχει, μεταξύ άλλων, την ομώνυμη πλατφόρμα κοινωνικής δικτύωσης Facebook.

[14] Martin, B. (2022) 'Privacy in a Programmed Platform: How the General Data Protection Regulation Applies to the Metaverse', *Harvard Journal of Law & Technology*, 36(1), σ. 235-261. Διαθέσιμο στο: https://jolt.law.harvard.edu/assets/articlePDFs/v36/Martin-Privacy-in-a-Programmed-Platform.pdf, σ. 243.

[15] Zuckerberg, M. (2021) 'Founder's Letter, 2021', *Meta*, 28 Οκτωβρίου. Διαθέσιμο στο: https://about.fb.com/news/2021/10/founders-letter/ [Πρόσβαση 5 Μαΐου 2023].

[16] Analysis and Research Team (ART) (2022) *Metaverse - Virtual World, Real Challenges*. Βρυξέλλες: Συμβούλιο της Ευρωπαϊκής Ένωσης. Διαθέσιμο στο: https://www.consilium.europa.eu/media/54987/metaverse-paper-9-march-2022.pdf, σ. 3.

2005. Για το λόγο αυτό, μέχρι σήμερα, δεν έχει αποκρυσταλλωθεί ένας καθολικά αποδεκτός εννοιολογικός ορισμός για το Metaverse[17].

Ο Zuckerberg χαρακτηρίζει το Metaverse ως ένα «*ενσαρκωμένο Διαδίκτυο*» *(embodied Internet)* που, σε αντίθεση με το σύγχρονο Διαδίκτυο, θα χαρίζει στους χρήστες μια «*βαθιά αίσθηση παρουσίας*» *(deep feeling of presence)*[18]· ο Διευθύνων Σύμβουλος της CoinBase, Brian Armstrong, το ορίζει ως την «*μακρινή εξέλιξη του WEB 3.0*» *(the distant evolution of Web3)*[19]· το Συμβούλιο της ΕΕ το περιγράφει ως έναν «*εμβυθιστικό, συνεχή και τρισδιάστατο εικονικό κόσμο, εντός του οποίου οι άνθρωποι αλληλεπιδρούν μέσω ενός άβαταρ, με σκοπό να ψυχαγωγηθούν, να πραγματοποιήσουν αγορές και να εκτελέσουν συναλλαγές με κρυπτογραφημένα περιουσιακά στοιχεία ή να εργασθούν δίχως να εγκαταλείψουν τη θέση τους*»[20].

Το Metaverse αντιπροσωπεύει ένα «*νέο σύνορο στην ανθρώπινη αλληλεπίδραση και το εμπόριο*» *(new frontier in human interaction and commerce)*[21] ή συμβολίζει, πιο γλαφυρά, το «*άγιο δισκοπότηρο των κοινωνικών συναλλαγών*» *(holy grail of social interactions)*[22]. Έρευνα του Gardner δείχνει ότι μόλις το 2026, το 25% των ανθρώπων θα αφιερώνει κατ' ελάχιστον μία ώρα ημερησίως για να εργασθεί, να ψωνίσει, να εκπαιδευτεί, να κοινωνικοποιηθεί ή/και να διασκεδάσει στο Metaverse[23].

Οι χρήστες θα συμμετέχουν στον εικονικό, 3D και σύγχρονο κόσμο του Metaverse υπό μορφή άβαταρ, από οποιαδήποτε γωνιά του πλανήτη, μέσω πληθώρας πλατφορμών

---

[17] Ό.π., Aamir (2022), σ. 8.

[18] Sanford, C. (2021) 'Meta (Facebook) Connect 2021 Metaverse Event Transcript', *Rev*, 29 Οκτωβρίου. Διαθέσιμο στο: https://www.rev.com/blog/transcripts/meta-facebook-connect-2021-metaverse-event-transcript [Πρόσβαση 5 Μαΐου 2023].

[19] Ό.π., Aamir (2022), σ. 7.

[20] Ό.π., Analysis and Research Team (ART) (2022).

[21] Kalyvaki, M. (2023) 'Navigating the metaverse business and legal challenges: Intellectual property, privacy, and jurisdiction', *Journal of Metaverse*, 3(1), σ. 87-92. Διαθέσιμο στο: https://doi.org/10.57019/jmv.1238344, σ. 87.

[22] Ό.π., Analysis and Research Team (ART) (2022).

[23] Gartner (2022) *Gartner Predicts 25% of People Will Spend At Least One Hour Per Day in the Metaverse by 2026*. Διαθέσιμο στο: https://www.gartner.com/en/newsroom/press-releases/2022-02-07-gartner-predicts-25-percent-of-people-will-spend-at-least-one-hour-per-day-in-the-metaverse-by-2026 [Πρόσβαση 23 Μαΐου 2023].

που θα λειτουργούν ως πύλες εισόδου *("portals")* σε αυτό[24]. Ο επιχειρηματίας Mathew Ball βαφτίζει τις εικονικές πλατφόρμες *"metagalaxies"*, παραλληλίζοντάς τες με τους γαλαξίες που συνθέτουν το υλικό Σύμπαν[25]. Η είσοδος όμως των χρηστών στο, κατά τα άλλα, άυλο Metaverse θα υλοποιείται με τη βοήθεια απτών συσκευών *("physical devices")*[26], ιδίως ειδικού εξοπλισμού εμβύθισης εικονικής ή επαυξημένης πραγματικότητας[27], επεξεργαστών υπολογιστών (CPUs) και δικτύων[28].

Το Metaverse θα χτιστεί επί τη βάσει ήδη γνωστών και προηγμένων τεχνολογιών (XR, IoT, AI, Blockchain, 5G, Cloud κ.ά.) και θα τρέφεται από Μεγάλα Δεδομένα (Big Data)[29]· μεσοπρόθεσμα, θα ενσωματώσει νέα τεχνολογικά εργαλεία που θα γεννώνται λόγω της επιστημονικής προόδου, ενισχύοντας τις δυνατότητές του, αλλά ταυτόχρονα οξύνοντας τις προκλήσεις που θα απορρέουν από την υλοποίησή του[30].

Το γεγονός ότι το Metaverse θα συντεθεί καταρχήν επί τη βάσει ανεπτυγμένων τεχνολογιών έχει οδηγήσει ορισμένους συγγραφείς να μη το αντιμετωπίζουν αυτό καθ' εαυτό ως μια νέα τεχνολογία, αλλά ως *«έναν νέο τρόπο αλληλεπίδρασης του χρήστη με τις ψηφιακές τεχνολογίες, τις πλατφόρμες και τις ψηφιακές υπηρεσίες, αλλά και με άλλους χρήστες»*[31], γνώμη την οποία συμμερίζεται και η γράφουσα.

Εντέλει, το Metaverse δεν είναι προς το παρόν παρά μια ιδέα[32] για την επέκταση της ανθρώπινης δραστηριότητας σε έναν παράλληλο και εμβυθιστικό εικονικό κόσμο, ως μετεξέλιξη του Διαδικτύου. Η κοινωνιολογική μετάβαση από την προ του Metaverse στη

---

[24] Κατ' αντιστοιχία των ιστοτόπων (websites) και ιστοσελίδων (webpages) που φιλοξενούνται και παρέχουν σήμερα πρόσβαση στον Παγκόσμιο Ιστό (βλ. ό.π., Aamir (2022), σ. 11).

[25] Kalpokas, I. and Kalpokienė, J. (2023) *Regulating the Metaverse: A Critical Assessment*. London: Routledge, σ. 5.

[26] Ό.π., Aamir (2022), σ. 12.

[27] European Parliamentary Research Service (EPRS) (2022) *Metaverse: Opportunities, risks and policy implications.* Βρυξέλλες: Ευρωπαϊκό Κοινοβούλιο. Διαθέσιμο στο: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733557/EPRS_BRI(2022)733557_EN.pdf, σ. 2.

[28] Ό.π., Aamir (2022).

[29] Chen, Z. et al. (2022) 'Metaverse Security and Privacy: An Overview', *2022 IEEE International Conference on Big Data (Big Data).* Διαθέσιμο στο: https://doi.org/10.1109/bigdata55660.2022.10021112, σ. 1.

[30] Ό.π., Di Pietro and Cresci (2021) σ. 283.

[31] Κουσουνή-Πανταζοπούλου, Α. (2023) 'Metaverse και αναφυόμενα νομικά ζητήματα' *Ελληνική Δικαιοσύνη, 2/2023,* σ. 377.

[32] Murphy, S. et al. (2021) 'The Metaverse: The evolution of a universal digital platform', *Norton Rose Fulbright*. Διαθέσιμο στο: https://www.nortonrosefulbright.com/en/knowledge/publications/5cd471a1/the-metaverse-the-evolution-of-a-universal-digital-platform [Πρόσβαση 5 Μαΐου 2023].

μετά το Metaverse εποχή θα επισυμβεί σταδιακά και τα όρια μεταξύ των δύο θα παραμείνουν ως επί το πλείστον δυσδιάκριτα[33]. Άλλωστε, δεν αποτελεί κατ' ουσίαν έναν προορισμό (*"The Metaverse is not a destination"*), αλλά μάλλον ένα σημείο στο χρόνο (*"but rather a point-in-time"*), στο οποίο οι άνθρωποι θα προσδίδουν μεγαλύτερη αξία στα εικονικά παρά στα υλικά αγαθά[34]. Σύμφωνα με εκτιμήσεις, η χρονική αυτή στιγμή απέχει μόλις δέκα με δεκαπέντε έτη από σήμερα[35].

2. Η ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΤΟΥ METAVERSE

2.1 Κύρια χαρακτηριστικά

Για να κατανοήσουμε βαθύτερα την ιδέα του Metaverse, ως μετεξέλιξης του Διαδικτύου που θα ενσωματώνει και θα συνδυάζει πολλές καινοτόμες τεχνολογίες, είναι κρίσιμο να αναλύσουμε τα βασικά χαρακτηριστικά που εικάζεται ότι μελλοντικά θα προσλάβει.

Ειδικότερα, το Metaverse θα είναι ένα περιβάλλον:

1. Εικονικό (virtual) και επιγραμμικό (online)[36]: δεν θα έχει υλική υπόσταση· θα προσομοιώνεται από και θα ζει μέσα σε υπολογιστικές μηχανές ως άυλο δημιούργημα, ενώ η συμμετοχή σε αυτό θα προϋποθέτει σύνδεση του χρησιμοποιούμενου εξοπλισμού στο Διαδίκτυο.

2. Εμβυθιστικό (immersive) και τρισδιάστατο (three-dimensional/3D): Ενώ στον ψηφιακό κόσμο του Διαδικτύου ο χρήστης πλοηγείται *επί του δικτύου*, στο Metaverse θα ταξιδεύει *εντός του δικτύου*[37], θα εμ-βυθίζεται δηλαδή χωρίς παρεμβολές (seamlessly) σε ένα εικονικό σύμπαν τριών διαστάσεων, όμοιο εν πολλοίς με το πραγματικό ("*immersive realism*"[38]). Ως εκ τούτου, το σώμα του θα ανταποκρίνεται στα εικονικά ερεθίσματα σαν να

---

[33] Ό.π.

[34] Ό.π., Citi GPS: Global Perspectives & Solutions (2022), σ. 17.

[35] Ό.π., Analysis and Research Team (ART) (2022), σ. 7.

[36] Ό.π., Aamir (2022), σ. 1.

[37] Kevins, J. (2022) 'Metaverse as a New Emerging Technology: An Interrogation of Opportunities and Legal Issues: Some Introspection', *SSRN Electronic Journal*. 9 Μαρτίου. Διαθέσιμο στο: https://doi.org/10.2139/ssrn.4050898, σ. 2.

[38] Wang, Y. *et al.* (2022) 'A survey on Metaverse: Fundamentals, Security, and Privacy', *IEEE Communications Surveys & Tutorials*, 25(1), σ. 319–352. Διαθέσιμο στο: https://doi.org/10.1109/comst.2022.3202047, σ. 324.

είναι αληθινά, ενώ ακόμη κι οι μνήμες που θα ανασύρει από την εικονική εμπειρία θα αναβιώνουν την έντονη αίσθηση (της πνευματικής και χωρικής)[39] παρουσίας που θα τον κατακλύζει στο Metaverse[40].

3. Συνεχές (persistent) και σύγχρονο (synchronous/live)[41]: Ο χρόνος στο Metaverse θα κυλάει γραμμικά, χωρίς δυνατότητα παύσης, επιστροφής στο παρελθόν ή μετάβασης στο μέλλον, και επ' αόριστον[42]. Η εικονική ζωή θα εκτυλίσσεται, λοιπόν, ακόμη και μετά την οριστική ή προσωρινή αποσύνδεση του χρήστη. Επιπλέον, όσα συμβαίνουν στο Metaverse θα αναμεταδίδονται στο χρήστη σε πραγματικό χρόνο (real-time)[43].

4. Απέραντης ισχύος (scalable)[44] και χωρητικότητας (massive)[45] : Καταργώντας τους φραγμούς του χωροχρόνου, το Metaverse υπόσχεται μια εμπειρία διαμοιραζόμενη ακώλυτα και ταυτόχρονα σε τεράστιο αριθμό τελικών χρηστών και τερματικών συσκευών ανά τον κόσμο (shared temporality/spatiality)[46], που θα βιώνεται εντός ενός εικονικού κόσμου αληθινών διαστάσεων.

Πέραν τούτων, *φιλοδοξείται* να είναι:

5. Ανοιχτό (open/inclusive)[47] και διαλειτουργικό (interoperable)[48]: Οποιοσδήποτε θα μπορεί να συμμετέχει στο Metaverse ελεύθερα (permissionlessly), ενώ το σχετικό υλισμικό (hardware) και λογισμικό (software) θα διαλειτουργούν. Ο χρήστης θα εμβυθίζεται στο εικονικό περιβάλλον χρησιμοποιώντας όποιο σετ εξοπλισμού επιθυμεί, ενώ η εικονική ταυτότητα, τα προσωπικά δεδομένα και τα περιουσιακά στοιχεία του θα μεταφέρονται απρόσκοπτα μεταξύ των διάφορων εμπειριών και πλατφορμών, χαρίζοντάς του μια

---

[39] Kim, Y. (2022) 'Virtual Reality Data and Its Privacy Regulatory Challenges: A Call to Move Beyond Text-Based Informed Consent', *California Law Review*, 110(2), σ. 225-256. Διαθέσιμο στο: https://doi.org/10.15779/Z380Z70X6P, σ. 233.

[40] Ό.π., Kalpokas, I. and Kalpokienė, J. (2023), σ. 21.

[41] Nextrope (2022) 'The State of The Metaverse in 2022 – Building in Open World'. Διαθέσιμο στο: https://nextrope.com/wp-content/themes/nextrope/assets/files/metaverse.pdf, σ. 9.

[42] Ό.π.

[43] Ό.π.

[44] Ό.π., European Parliamentary Research Service (EPRS) (2022), σ. 2.

[45] Ό.π., Analysis and Research Team (ART) (2022), σ. 3.

[46] Nevelsteen, K.J. (2017) 'Virtual World, Defined from a Technological Perspective, and Applied to Video Games, Mixed Reality and the Metaverse', *Computer Animation and Virtual Worlds*, 29(1). Διαθέσιμο στο: https://doi.org/10.1002/cav.1752, σ. 7-8.

[47] Ό.π., Nextrope (2022).

[48] Ό.π.

δυναμική και άκρως συμμετοχική εμπειρία[49], σε αντίθεση με ό,τι συμβαίνει σήμερα στο κατακερματισμένο ψηφιακό περιβάλλον του WEB 2.0.

Ταυτόχρονα, το Metaverse θα αποτελέσει:

6. Σύζευξη υλικού και εικονικού κόσμου (*"phygital world"*)[50]: Στο Metaverse, που κατασκευάζεται κατ' εικόνα και καθ' ομοίωση του πραγματικού κόσμου, οι εμπειρίες και τα ερεθίσματα του χρήστη θα μοιάζουν σε μεγάλο βαθμό αληθινά. Ο ίδιος θα μπορεί να επικοινωνεί μέσω της ομιλίας και της γλώσσας του σώματος, να κινείται απεριόριστα στο χώρο και να αφουγκράζεται το περιβάλλον του μέσω της όρασης, της ακοής[51] και εν μέρει της αφής, ενδεχομένως, δε, στο μέλλον μέσω του πλήρους φάσματος των ανθρώπινων αισθήσεων[52]. Παράλληλα, οι δραστηριότητες που θα προσφέρει ο εικονικός κόσμος θα αντλούνται από την καθημερινή ζωή αναπαράγοντάς την, επιτρέποντας στους χρήστες «*να εργαστούν, να ψυχαγωγηθούν, να αναπαυθούν, να πραγματοποιήσουν συναλλαγές και να κοινωνικοποιηθούν*[53]» εικονικά. Η απόλυτη σύζευξη πραγματικότητας και εικονικότητας θα επιτευχθεί, όμως, μόνο υπό τον όρο της ευρείας, αδιάλειπτης και σύγχρονης συλλογής και επεξεργασίας δεδομένων των (άψυχων και έμψυχων) στοιχείων του φυσικού κόσμου και της συνακόλουθης ρεαλιστικής απόδοσής τους από το Metaverse (Big Data[54] σε ενισχυμένη μορφή).

---

[49] Ήδη έχει δημιουργηθεί το Metaverse Standards Forum, ως ένα φόρουμ συνεργασίας μεταξύ πλείστων ενδιαφερόμενων μερών, με κοινό στόχο την ανάπτυξη και καθιέρωση προτύπων διαλειτουργικότητας στο Metaverse περιβάλλον (βλ. Metaverse Standards Forum (2023). The Metaverse Standards Forum. Διαθέσιμο στο: https://metaverse-standards.org/ [Πρόσβαση 6 Μαΐου 2023]).

[50] Συγκερασμός των αγγλικών όρων physical και digital (βλ. ό.π., Analysis and Research Team (ART) (2022), σ. 3).

[51] Σύμφωνα με τον Luciano Floridi, το Metaverse μπορεί να προσφέρει μια δυσδιάστατη (*"bidimensional"*) αισθητηριακή εμπειρία, σε αντίθεση με την αναλογική πραγματικότητα, την οποία ο άνθρωπος προσεγγίζει και με τις πέντε αισθήσεις (βλ. Floridi, L. (2022) 'Metaverse: a Matter of Experience', *SSRN Electronic Journal*. 13 Ιουνίου. Διαθέσιμο στο: https://doi.org/10.2139/ssrn.4121411, σ. 3).

[52] Με την έλευση των δικτύων 6G και του Διαδικτύου των Αισθήσεων (βλ. ό.π., Analysis and Research Team (ART) (2022), σ. 4).

[53] JPMorgan Chase & Co (2022) 'Opportunities in the metaverse'. Διαθέσιμο στο: https://www.jpmorgan.com/content/dam/jpm/treasury-services/documents/opportunities-in-the-metaverse.pdf , σ. 3.

[54] Ο όρος αναφέρεται σε σύνολα δεδομένων, τόσο ογκώδη και περίπλοκα, που εκφεύγουν από τις δυνατότητες των παραδοσιακών μεθόδων επεξεργασίας δεδομένων.

7. Ανεξάρτητη οικονομία *("a fully functioning economy")*[55]: Το Metaverse θα είναι ένα αυτοσυντηρούμενο οικοσύστημα με τη δική του εικονική οικονομία ("*virtual economy*"), εσωτερική οικονομική διακυβέρνηση ("*internal economic governance*"), σύστημα εμπορικών ("*commerce*") και οικονομικών συναλλαγών ("*trading system*"), αλλά και κανόνες ιδιοκτησίας ("*ownership*")[56]. Οι συμμετέχοντες, είτε είναι φυσικά ή νομικά πρόσωπα, θα μπορούν να δημιουργούν και να κατέχουν αξία (value), να επενδύουν και να συναλλάσσονται μέσω κρυπτοπαραστατικών αξίας (πχ. κρυπτονομισμάτων, NFTs κ.ο.κ.), που θα αναγνωρίζονται ως ισχυρά από τους ομότιμους χρήστες του δικτύου[57].

8. Περαιτέρω, ο τελικός χρήστης θα αλληλεπιδρά με τους υπόλοιπους χρήστες - είτε είναι άνθρωποι είτε bots, δηλαδή εικονικοί πράκτορες Τεχνητής Νοημοσύνης (automated, AI-based virtual agents)[58] - και με το περιβάλλον του, μέσω ενός άβαταρ[59]· μιας εικονικής δηλαδή αναπαράστασης του εαυτού του σε τρισδιάστατη μορφή[60], ενός ρεαλιστικού ψηφιακού ομοιώματος[61] που θα προβάλλει με ακρίβεια τον προσανατολισμό, τη στάση και τις κινήσεις του σώματός του, αλλά και τις κινήσεις του κεφαλιού και τις εκφράσεις του προσώπου του στον εικονικό κόσμο. Ο χρήστης θα δημιουργεί το άβαταρ αυτό αμέσως μετά την είσοδό του στο Metaverse και θα μπορεί να επιλέξει ελεύθερα τη μορφή[62] και τα

---

[55] Ό.π., Nextrope (2022).

[56] Ό.π., Sandeepa, C., Wang, S. and Liyanage M. (2023), σ. 2.

[57] Συνδυαστικά, αλλά ειδικά σε πλατφόρμες με κεντρικό έλεγχο, οι συναλλαγές θα μπορούν να διεκπεραιώνονται και/ιδίως μέσω παραστατικού χρήματος (fiat currency) (πχ. Ευρώ, Δολάριο κ.ο.κ), εγγενών ψηφιακών νομισμάτων (in-game digital currency) (πχ. Robux, V-Bucks κ.ο.κ.), stablecoins ή Ψηφιακού Νομίσματος Κεντρικής Τράπεζας (Central Bank Digital Currency/CBDC) (πχ. CBDC Νιγηρίας, Κίνας κ.ο.κ) (βλ. Deloitte Canada (n.d.) 'Welcome to the Metaverse'. Διαθέσιμο στο: https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/technology-media-telecommunications/ca-industry-tmt-welcome-to-the-metaverse-en.pdf, σ. 21 και ό.π., Citi GPS: Global Perspectives & Solutions (2022), σ. 15).

[58] Στο Metaverse, ως άβαταρ θα μπορούν να συμμετέχουν τόσο οι πραγματικοί χρήστες όσο και εικονικοί πράκτορες Τεχνητής Νοημοσύνης (βλ. ό.π., Kalpokas, I. and Kalpokienė, J. (2023), σ. 16).

[59] Στα σανσκριτικά και τον Ινδουισμό, «άβαταρ» σημαίνει την υλική εμφάνιση ή την ενσάρκωση μιας θεότητας στη Γη (βλ. Βικιπαίδεια (2022) *Άβαταρ*. Διαθέσιμο στο: https://el.wikipedia.org/wiki/%CE%86%CE%B2%CE%B1%CF%84%CE%B1%CF%81 [Πρόσβαση 6 Μαΐου 2023]).

[60] Χιόνη, Γ. (2022) 'Δίκαιο και Μετασύμπαν (ΙΙ): Το δίκαιο των avatar', *Lawspot*, 12 Οκτωβρίου. Διαθέσιμο στο: https://www.lawspot.gr/nomika-blogs/georgia_hioni/dikaio-kai-metasympan-ii-dikaio-ton-avatar [Πρόσβαση 6 Μαΐου 2023]).

[61] Bolognini, L. and Carpenelli, M. E. (2022) 'The future of personal data in the Metaverse', *Zenodo*. Διαθέσιμο στο: https://doi.org/10.5281/zenodo.6413046, σ. 2.

[62] Ό.π., European Parliamentary Research Service (EPRS) (2022), σ. 2.

φυσικά[63] και κοινωνικά[64] χαρακτηριστικά του. Τα εξατομικευμένα άβαταρ (customized avatars) θα προσφέρουν έτσι στους χρήστες μια ισχυρή αίσθηση μοναδικότητας και (εικονικής) ταυτότητας (virtual identity)[65]. Ως τέτοια (i.e., εξατομικευμένα), θα είναι ένας συνδυασμός υπολογιστικού κώδικα (*"code"*), εμφάνισης (*"appearance"*), δεδομένων που τα αφορούν (*"associated data"*) και αντικειμένων (*"belongings"*) που φέρουν[66]. Υποστηρίζεται και ότι ο χρήστης θα μπορεί να έχει περισσότερα από ένα άβαταρ στο Metaverse και άρα, πάνω από μια εικονικές ταυτότητες ή και προσωπικότητες[67].

9. Τέλος, η υποστήριξη της βαριάς υποδομής του Metaverse προϋποθέτει αφενός, την αύξηση της διαθέσιμης υπολογιστικής ισχύος (απαιτείται η πρόσβαση σε petaflops ανά χιλιοστό του δευτερολέπτου[68] για την απόδοση των 3D εικονικών εμπειριών σε πραγματικό χρόνο χωρίς καθυστέρηση – low latency), της χωρητικότητας αποθήκευσης δεδομένων, των ταχυτήτων σύνδεσης και της κατανάλωσης ενέργειας[69], και αφετέρου, τη σύγκλιση υφιστάμενων και εκκολαπτόμενων, εξελιγμένων τεχνολογιών (*"the convergence of a range of nascent and extant digital and online technologies"*[70]), οι οποίες, ως συγκολλητική ουσία του Metaverse, θα συνθέσουν την υποδομή, θα παρέχουν την πρόσβαση και θα επιτρέψουν την ομαλή και αυτόνομη λειτουργία του.

2.2 Τεχνολογίες αιχμής

Στην ενότητα αυτή, θα επιχειρήσουμε μια συνοπτική ανάλυση των καίριων εκείνων τεχνολογιών που μαζί με άλλες θα επιτρέψουν τη διέλευσή μας από την εποχή του Internet και του Διαδικτύου των Πραγμάτων (Internet of Things/IoT) στην εποχή του Metaverse και του Διαδικτύου των Αισθήσεων (Internet of Senses/IoS)[71].

---

[63] Π.χ. χρώμα ματιών, μαλλιών, ύψος, βιολογικό φύλο κ.ο.κ.

[64] Π.χ. καταγωγή, επάγγελμα, ταυτότητα φύλου κ.ο.κ.

[65] Ό.π., Chen, Z. et al. (2022), σ. 2.

[66] Ό.π., Kalpokas, I. and Kalpokienė, J. (2023), σ. 108.

[67] Ό.π., Citi GPS: Global Perspectives & Solutions (2022), σ. 42. Τελικά, η επιλογή θα εξαρτηθεί από διάφορους παράγοντες, μεταξύ των οποίων η πολιτική ή το μοντέλο διακυβέρνησης της κάθε πλατφόρμας.

[68] Ό.π., Nextrope (2022), σ. 14.

[69] Ό.π., Kalpokas, I. and Kalpokienė, J. (2023), σ. 18.

[70] Ό.π., Murphy, S. et al. (2021).

[71] Πρόκειται για ένα διαδικτυακό οικοσύστημα, εντός του οποίου ο χρήστης θα μπορεί να βιώσει αισθητηριακές εμπειρίες, με τη βοήθεια της νευροδιέγερσης, δικτύων 6G και λοιπών τεχνολογιών (βλ. Castro, C. (2021) 'Tasting Digital: How the Way you Sense the World Will Change in the Next

1. Εικονική Πραγματικότητα (Virtual Reality/VR): τεχνολογία 3D προσομοίωσης ενός πραγματικού ή φαντασιακού κόσμου από έναν υπολογιστή, η οποία περικλείει ισότιμα εξειδικευμένο λογισμικό και υλισμικό. Ειδικότερα, η εμβύθιση του χρήστη στην εικονική εφαρμογή και η αποσύνδεσή του από το φυσικό περιβάλλον πραγματοποιείται με τη χρήση ειδικού εξοπλισμού συνδεόμενου στο Διαδίκτυο, που περιλαμβάνει - προς το παρόν - είτε διατάξεις κεφαλής Εικονικής Πραγματικότητας (VR headsets)[72] είτε περιβάλλοντα πολλαπλών προβολών (multi-projected environments)[73].

Decade', *6GWorld*, 7 Ιανουαρίου. Διαθέσιμο στο: https://www.6gworld.com/exclusives/tasting-digital-how-the-way-you-sense-the-world-will-change-by-the-time-6g-is-real/ [Πρόσβαση 12 Μαΐου 2023].

[72] Βασικά απαρτίζονται από μια διάταξη οπτικής προβολής προσαρτώμενη στο κεφάλι (Head-mounted Display/HMD) και μια μικρή οθόνη τοποθετούμενη μπροστά από κάθε μάτι (βλ. Vergara, D., Rubio, M.P. and Lorenzo, M. (2017) 'On the Design of Virtual Reality Learning Environments in Engineering', *Multimodal Technologies and Interaction*, 1(2). Διαθέσιμο στο: https://doi.org/10.3390/mti1020011, σ. 2). Διαθέτουν, εκτός των άλλων (πχ. επεξεργαστή, κάρτα γραφικών, κάρτα μνήμης, μπαταρία, WiFi, Bluetooth κλπ.), ενσωματωμένες κάμερες, ηχεία και λοιπούς αισθητήρες για την αναγνώριση της κατεύθυνσης, της στάσης και των κινήσεων του σώματος και του κεφαλιού (pose/body/head tracking technology) του χρήστη, ενίοτε δε, για την αναγνώριση των κινήσεων των ματιών, της κατεύθυνσης του βλέμματος και των εκφράσεων του προσώπου του (eye/gaze/face tracking technology). Συχνά περιλαμβάνουν και τηλεχειριστήρια (controllers), μηχανισμούς αναγνώρισης της κίνησης των χεριών και των δαχτύλων (hand/finger tracking) ή χρησιμοποιούνται συνδυαστικά με μηχανισμούς ανάδρασης μέσω απτικής τεχνολογίας (haptic technology), όπως απτικά γάντια (haptic gloves) ή απτικές στολές (haptic suits). Τέλος, αν και η τεχνολογία διεπαφής εγκεφάλου – υπολογιστή (Brain-Computer Interface) δεν χρησιμοποιείται ακόμη στις καταναλωτικές συσκευές VR, ενδέχεται να απελευθερώσει το πεδίο της Εικονικής Πραγματικότητας, συνδέοντας απευθείας τα εγκεφαλικά σήματα του χρήστη με την εικονική εφαρμογή. Προς το παρόν περιλαμβάνει αισθητήρες ηλεκτροεγκεφαλογραφίας (EEG) που τοποθετούνται στο κεφάλι, ενώ μελλοντικά μπορεί να εξελιχθεί σε νευρωνικά εμφυτεύματα. Βλ. Dick, E. (2021) 'Balancing user privacy and innovation in Augmented and Virtual Reality', *Information Technology and Innovation Foundation*, 4 Μαρτίου. Διαθέσιμο στο: https://itif.org/publications/2021/03/04/balancing-user-privacy-and-innovation-augmented-and-virtual-reality/ [Πρόσβαση 14 Μαΐου 2023], Wikipedia (2023) *Virtual reality.* Διαθέσιμο στο: https://en.wikipedia.org/wiki/Virtual_reality [Πρόσβαση 12 Μαΐου 2023], Wikipedia (2023) *Virtual reality headset*. Διαθέσιμο στο: https://en.wikipedia.org/wiki/Virtual_reality_headset [Πρόσβαση 12 Μαΐου 2023] και ό.π. Nextrope (2022), σ. 20.

[73] Βλ. το CAVE (Cave Automatic Virtual Environment), ένα περιβάλλον Εικονικής Πραγματικότητας, που αποτελείται από ένα δωμάτιο σε σχήμα κύβου, στο οποίο οι τοίχοι, το πάτωμα και το ταβάνι αποτελούν οθόνες οπτικής απεικόνισης του εικονικού κόσμου μέσω στερεοσκοπικών προβολέων. Η εμβύθιση του χρήστη επιτυγχάνεται μέσω παθητικών 3D γυαλιών, που δημιουργούν την ψευδαίσθηση των τριών διαστάσεων, χωρίς επεξεργασία προσωπικών δεδομένων του φορέα (βλ. ό.π., Vergara, D., Rubio, M.P. and Lorenzo, M. (2017)). Για το λόγο αυτό, εκφεύγει του πεδίου μελέτης της παρούσας.

Ο υποψήφιος χρήστης του Metaverse θα μπορεί να χρησιμοποιεί το υλισμικό της τεχνολογίας VR (κατ' αρχήν, μία διάταξη κεφαλής VR, η οποία σταδιακά θα μετεξελιχθεί σε πιο απλά και ελαφριά γυαλιά VR[74]), αντί για τις 2D οθόνες του WEB 2.0, προκειμένου να εμβυθιστεί στο 3D οικοσύστημα. Ο εξοπλισμός VR θα περιέχει ένα κατάστημα εφαρμογών (app store), από το οποίο ο χρήστης θα κατεβάζει τη σχετική Metaverse εφαρμογή[75]. Με την είσοδό του στην 3D πλατφόρμα, θα μπορεί να παρατηρήσει σφαιρικά τον εικονικό κόσμο, να περιηγηθεί εντός του και να αλληλεπιδράσει με άλλους χρήστες ή εικονικά αντικείμενα (virtual objects), ενώ χρησιμοποιώντας και το υλισμικό της απτικής τεχνολογίας, θα μπορεί να προσεγγίσει το εικονικό περιβάλλον και με την αίσθηση της αφής[76]. Η διάταξη κεφαλής VR Oculus Quest του ομίλου Meta Platforms αποτελεί τον πιο δημοφιλή εξοπλισμό Εικονικής Πραγματικότητας[77], ενώ εξαιρετικό τεχνολογικό ενδιαφέρον παρουσιάζει και η ολόσωμη στολή με απτική ανατροφοδότηση Teslasuit της Tesla.

2. Μεικτή Πραγματικότητα (Mixed Reality/MR)[78] [79]: τεχνολογία σύζευξης του πραγματικού με τον εικονικό κόσμο, που αλληλεπιδρούν σε πραγματικό χρόνο και σε τρεις διαστάσεις[80]. Διακρίνεται στην Επαυξημένη Πραγματικότητα (Augmented Reality/AR), δηλαδή την επικάλυψη της πραγματικής από την ψηφιακή ζωή (ένα ψηφιακό υπόστρωμα – [πληροφοριών ή/και αντικειμένων] επικάθεται στον φυσικό κόσμο[81]), αλλά και την Επαυξημένη Εικονικότητα (Augmented Virtuality/AV), δηλαδή την ενσωμάτωση φυσικών στοιχείων στο εικονικό περιβάλλον για την ενίσχυση και τον εμπλουτισμό της εικονικής εμπειρίας[82]. Η εν λόγω τεχνολογία περιλαμβάνει εξειδικευμένο λογισμικό και υλισμικό. Η επαύξηση της πραγματικότητας ή αντίστοιχα, η ενίσχυση της εικονικότητας υλοποιείται

[74] Ό.π., Aamir, O. (2022), σελ. 12.

[75] Nair, V., Garrido, G.M. and Song, D. (2022) 'Exploring the Unprecedented Privacy Risks of the Metaverse', *arXiv (Cornell University)*. Διαθέσιμο στο: https://doi.org/10.48550/arXiv.2207.13176, σ. 2.

[76] Lim, W.M. et al. (2022) 'Realizing the Metaverse with Edge Intelligence: A Match Made in Heaven' IEEE Wireless Communications, σ. 1–9. Διαθέσιμο στο: https://doi.org/10.1109/mwc.018.2100716, σ. 2

[77] Garrett, U. (2023) 'Why the Meta Quest 2 is still the virtual reality headset to buy', *CNN Underscored*. 24 Ιανουαρίου. Διαθέσιμο στο: https://edition.cnn.com/cnn-underscored/reviews/oculus-quest-2 [Πρόσβαση 23 Μαΐου 2023]

[78] Ο όρος χρησιμοποιείται συχνά ως συνώνυμος της Επαυξημένης Πραγματικότητας.

[79] Η Εικονική και η Μεικτή Πραγματικότητα αποτελούν συνιστώσες της λεγόμενης «Εκτεταμένης Πραγματικότητας» (Extended Reality/XR).

[80] Sebastian, G. (2023) 'A descriptive study on Metaverse', *International Journal of Security and Privacy in Pervasive Computing*, 15(1), σ. 1–14. Διαθέσιμο στο: https://doi:10.4018/ijsppc.315591, σ. 4.

[81] Ό.π., Bolognini, L. and Carpenelli, M. E. (2022), σ. 3.

[82] Ό.π., Sebastian, G. (2023).

με τη χρήση ειδικής συσκευής MR (πχ. έξυπνο τηλέφωνο, έξυπνα γυαλιά, HMD κ.ά.) συνδεόμενης στο Διαδίκτυο και εξοπλισμένης με κάμερα που ενσωματώνει λογισμικό MR[83] [84]. Το αποτέλεσμα είναι η δημιουργία στο χρήστη της ψευδαίσθησης ότι πρόκειται για ένα ενιαίο περιβάλλον. Η εφαρμογή Pokémon Go της Niantic, τα έξυπνα γυαλιά Google Glasses της Google και η διάταξη κεφαλής HoloLens της Microsoft αποτελούν χαρακτηριστικά παραδείγματα της εν λόγω τεχνολογίας.

Η χρήση εφαρμογών Μεικτής Πραγματικότητας θα μυήσει το χρήστη στο εικονικό περιβάλλον του Metaverse, χωρίς να τον αποσυνδέσει εντελώς από το φυσικό περιβάλλον. Σε κάθε περίπτωση, η τεχνολογία XR, είτε υπό μορφή VR είτε υπό μορφή MR, θα αποτελέσει το όχημα για την είσοδο των χρηστών στο θαυμαστό κόσμο του Metaverse, ενώ η απτική τεχνολογία αναμένεται να συμβάλει ουσιωδώς στην ενίσχυση της εμβύθισης, δημιουργώντας στους χρήστες τουλάχιστον την αίσθηση της πίεσης και της υφής[85].

3. Διαδίκτυο των Πραγμάτων (Internet of Things/IoT): τεχνολογία δυνάμει της οποίας συσκευές με μοναδικά αναγνωριστικά και ενσωματωμένους αισθητήρες (sensors) έχουν τη δυνατότητα, συνδεόμενες στο Διαδίκτυο, να ανταλλάσσουν πληροφορίες για τον φυσικό κόσμο με άλλες συσκευές, συστήματα ή δίκτυα χωρίς ανθρώπινη παρέμβαση[86].

Με την εν λόγω τεχνολογία, τα συνθετικά στοιχεία του υλικού κόσμου θα αναπαράγονται με ακρίβεια στο Metaverse, ώστε ο χρήστης να απολαμβάνει μια όσο το δυνατόν περισσότερο ρεαλιστική εμπειρία. Ενδεικτικά, συσκευές IoT θα χρησιμοποιούνται για την προσομοίωση των φυσικών καιρικών συνθηκών και των τεσσάρων εποχών στο εικονικό περιβάλλον[87]. Υπολογίζεται ότι μέχρι το 2025, ο συνολικός αριθμός των IoT συσκευών θα έχει αγγίξει τα 30,9 δισεκατομμύρια, σε αντίθεση με τα 13,8 δισεκατομμύρια διασυνδεδεμένων συσκευών που καταγράφηκαν το 2021[88].

---

[83] Βλ. ό.π., Nextrope (2022), σ. 20, που κάνει ειδική αναφορά στην τεχνολογία AR. Το λογισμικό AR αναγνωρίζει το αντικείμενο στο οποίο εστιάζει η κάμερα της συσκευής και κατόπιν, μεταφορτώνει σχετικές με αυτό πληροφορίες από το νέφος (Cloud), οι οποίες είτε εμφανίζονται αυτόματα στην οθόνη της συσκευής, είτε προβάλλονται αυτόματα στο φυσικό περιβάλλον. Κατ' αντίστοιχο τρόπο, δύναται να ψηφιοποιηθούν φυσικά αντικείμενα.

[84] Και η τεχνολογία MR μπορεί να ενσωματώνει μηχανισμούς και αισθητήρες που αξιοποιούνται από την τεχνολογία VR (βλ. υποσημείωση 71).

[85] Ό.π., Sebastian, G. (2023), σ. 4.

[86] Wikipedia (2023) *Internet of things*. Διαθέσιμο στο: https://en.wikipedia.org/wiki/Internet_of_things [Πρόσβαση 12 Μαΐου 2023].

[87] Ό.π., Nextrope (2022), σ. 23.

[88] Ό.π., Sebastian, G. (2023), σ. 5.

4. Τεχνητή Νοημοσύνη (Artificial Intelligence/AI): τεχνολογία *που «αναφέρεται σε* [υπολογιστικά] *συστήματα τα οποία χαρακτηρίζονται από ευφυή συμπεριφορά, αναλύοντας το περιβάλλον τους και ενεργώντας – με κάποιο βαθμό αυτονομίας – για την επίτευξη συγκεκριμένων στόχων»*[89] [90].

Η Τεχνητή Νοημοσύνη πρόκειται να κατέχει πρωταγωνιστικό ρόλο στο Metaverse, συλλέγοντας, αναλύοντας και αξιοποιώντας τα μαζικώς παραγόμενα στο εικονικό περιβάλλον δεδομένα (Big Data Analytics), μέσω αλγορίθμων μηχανικής (Machine Learning Algorithms/ML)[91] και βαθιάς μηχανικής μάθησης (Deep Learning Algorithms/DL)[92][93]. Οι εν λόγω αλγόριθμοι αναμένεται να ενσωματωθούν τόσο στον ειδικό εξοπλισμό εμβύθισης, όσο και στο λογισμικό της εικονικής εφαρμογής.

Ιδιαιτέρως σημαντικό θα αναδειχθεί το επιστημονικό πεδίο της Επεξεργασίας Φυσικής Γλώσσας (Natural Language Processing/NLP), το οποίο εστιάζει στην αναγνώριση, ανάλυση, κατανόηση και παραγωγή φυσικής γλώσσας[94], αυτό της Μηχανικής Όρασης

---

[89] Ανακοίνωση της Ευρωπαϊκής Επιτροπής, Τεχνητή Νοημοσύνη για την Ευρώπη, της 25ης Απριλίου 2018, COM (2018) 237 final, 25.04.2018.

[90] Η Τεχνητή Νοημοσύνη διακρίνεται σε Στενή ή Ασθενή (Narrow or Weak AI), που διαθέτει περιορισμένες ικανότητες, σε Γενική ή Ισχυρή (General or Strong AI), που διαθέτει αντίστοιχες νοητικές ικανότητες με τον άνθρωπο και στην Υπερευφυΐα ή Υπερνοημοσύνη (Superintelligence), που ξεπερνά την ανθρώπινη νοημοσύνη (βλ. Glover, E. (2022) 'Strong AI vs. Weak AI: What's the Difference?' *Built In*, 27 Οκτωβρίου. Διαθέσιμο στο: https://builtin.com/artificial-intelligence/strong-ai-weak-ai [Πρόσβαση 12 Μαΐου 2023]). Σήμερα, η τεχνολογία βρίσκεται στο επίπεδο της Στενούς ή Ασθενούς Τεχνητής Νοημοσύνης.

[91] Οι αλγόριθμοι μηχανικής μάθησης προγραμματίζονται και εκπαιδεύονται από τον άνθρωπο, ενώ διαθέτουν την ικανότητα να μαθαίνουν αυτόνομα, δηλαδή να προσαρμόζονται, να βελτιώνονται και να εξελίσσονται, χωρίς την ανάγκη εξωτερικής παρέμβασης και μεταβολής των κανόνων από τους οποίους διέπονται (βλ. Directorate-General for Justice and Consumers (2020) *Algorithmic discrimination in Europe: Challenges and opportunities for gender equality and non-discrimination law.* Λουξεμβούργο: Ευρωπαϊκή Επιτροπή. Διαθέσιμο στο: https://op.europa.eu/en/publication-detail/-/publication/082f1dbc-821d-11eb-9ac9-01aa75ed71a1/language-en, σ. 33).

[92] Πρόκειται για εξελιγμένη υποκατηγορία των αλγορίθμων μηχανικής μάθησης, που φιλοδοξούν να αντιγράψουν την πολύπλοκη λειτουργία και πολυεπίπεδη αρχιτεκτονική των νευρώνων του ανθρώπινου εγκεφάλου, χρησιμοποιώντας τα λεγόμενα «νευρωνικά δίκτυα» (neural networks). Στηρίζονται σε αδρομερή προγραμματισμό και εκπαίδευση. Αποτελούν σπουδαία εργαλεία για απαιτητικές εργασίες, όπως είναι η επεξεργασία φυσικής γλώσσας (πχ. αυτόματη μετάφραση, chatbots, εικονικοί βοηθοί, ανάλυση συναισθημάτων κ.ο.κ.) και η αναγνώριση και κατηγοριοποίηση εικόνας, ήχου και προσώπων (βλ. ό.π., σ. 36).

[93] Huynh-The, T. et al. (2023) 'Artificial intelligence for the metaverse: A survey', *Engineering Applications of Artificial Intelligence*, 117, 105581. Διαθέσιμο στο: https://doi.org/10.1016/j.engappai.2022.105581, σ. 2.

[94] Ό.π., σ. 5-6.

(Machine Vision), συμπεριλαμβανομένης της Υπολογιστικής Όρασης (Computer Vision), που εστιάζει στην ανίχνευση, ανάλυση και ερμηνεία δεδομένων από οπτικά περιβάλλοντα (πχ. ψηφιακές εικόνες, βίντεο κ.ά.) για την εξαγωγή υψηλού επιπέδου πληροφοριών[95], αλλά και η τεχνολογία Πρακτόρων Λογισμικού (Software Agent Technology), που αναφέρεται σε προγράμματα υπολογιστή Τεχνητής Νοημοσύνης που εκτελούν συνεχόμενα και αυτόνομα διάφορες ενέργειες, για λογαριασμό ενός ανθρώπου ή οργανισμού.

Με αυτόν τον τρόπο, η Τεχνητή Νοημοσύνη θα αποτελέσει αναγκαίο εργαλείο για τη βελτίωση της εμβυθιστικής εμπειρίας των χρηστών[96], της αλληλεπίδρασης μεταξύ τους, αλλά και της αλληλεπίδρασης μεταξύ χρηστών και bots[97], για την ανάλυση της γραπτής και προφορικής επικοινωνίας, της συμπεριφοράς και της γλώσσας του σώματός τους, για την αναγνώριση μοτίβων, την πρόβλεψη πιθανοτήτων, τη σκιαγράφηση ατομικού προφίλ και την αυτοματοποιημένη λήψη αποφάσεων, για τη δημιουργία προσωποποιημένων άβαταρ[98] και υπηρεσιών και γενικότερα τη ρεαλιστική και σύγχρονη απόδοση των φυσικών στοιχείων στον εικονικό κόσμο κ.ά[99].

5. Τεχνολογία Κατανεμημένου Καθολικού (Distributed Ledger Technology/DLT) ή αλλιώς Τεχνολογία Blockchain (εφεξής "Blockchain")[100]: τεχνολογία του WEB 3.0, η οποία επιτρέπει τη συνεχή καταγραφή, αναλλοίωτη αποθήκευση και εσαεί διατήρηση δεδομένων εντός οποιουδήποτε αποκεντρωμένου δικτύου. Τα δεδομένα εγγράφονται ομαδοποιημένα σε κωδικοποιημένα (hashed) και χρονικά αριθμημένα τμήματα, τις λεγόμενες «συστοιχίες» (blocks)[101], που κατανέμονται άρρηκτα σε αλυσίδα (chain)[102], ει μη μόνον με τη συναίνεση

---

[95] Ό.π., σ. 6-7.

[96] Ό.π., σ. 1.

[97] Ό.π., Nextrope (2022), σ. 21.

[98] Εστιάζοντας στα ιδιαίτερα χαρακτηριστικά προσώπου του χρήστη, πχ. μέσω σάρωσης 2D εικόνων (βλ. ό.π.).

[99] Η Τεχνητή Νοημοσύνη μπορεί, πχ., να δημιουργήσει τρισδιάστατα άβαταρ, τα εικονικά ρούχα των οποίων τσαλακώνονται όσο οι χρήστες κινούνται, αντικατοπτρίζοντας την κινητική δραστηριότητά τους με ρεαλιστικό τρόπο (βλ. Martin, B. (2022), σ. 247).

[100] Η έννοια της τεχνολογίας του Blockchain εισήχθη για πρώτη φορά το 2008, με τη δημοσίευση του "Bitcoin White Paper" από ένα άτομο ή μια ομάδα ανθρώπων με το ψευδώνυμο "Satoshi Nakamoto".

[101] Κάθε block ομαδοποιεί πολλαπλές συναλλαγές, που εγγράφονται στο δίκτυο μέσω της λεγόμενης «συνάρτησης κατακερματισμού», μιας κρυπτογραφικής λειτουργίας μονής κατεύθυνσης (one-way hash function), δυνάμει της οποίας συγκεκριμένα δεδομένα εισόδου (input) παράγουν μια μοναδική ακολουθία χαρακτήρων και αριθμών (string of characters and numbers), τη λεγόμενη «τιμή κατακερματισμού» (hash value), εν είδει μοναδικού ψηφιακού αποτυπώματος. Κάθε αλλαγή στο

των ομότιμων (peer-to-peer) χρηστών/κόμβων (nodes) του αποκεντρωμένου δικτύου. Ταυτόχρονα, κάθε χρήστης/κόμβος έχει πρόσβαση και αποθηκεύει ενημερωμένο αντίγραφο μέρους (lightweight nodes) ή του συνόλου (full nodes) της αλυσίδας εγγραφών[103] [104], έτσι ώστε η βλάβη ενός ή περισσότερων κόμβων να μην επηρεάζει την πρόσβαση στα δεδομένα. Κατ' αυτόν τον τρόπο, διασφαλίζεται αφενός, η ασφάλεια και η ανθεκτικότητα των δεδομένων και αφετέρου, η απαλλαγή από παντός είδους μεσάζοντες, που σηματοδοτεί τη μετάβαση από τους «περιφραγμένους κήπους[105]» (walled gardens) του WEB 2.0 στο ανοιχτό και αποκεντρωμένο περιβάλλον του WEB 3.0.

Περαιτέρω, το Blockchain μπορεί να λειτουργήσει είτε ως τεχνολογία αποθήκευσης δεδομένων είτε ως υποδομή για την εκτέλεση λογισμικού[106]. Χαρακτηριστικό παράδειγμα ειδικότερων εφαρμογών της τεχνολογίας του Blockchain αποτελούν τα (ανταλλάξιμα) κρυπτονομίσματα (cryptocurrencies/cryptos), τα μη εναλλάξιμα κρυπτοπαραστατικά (non-fungible tokens/NFTs), καθώς και οι Αποκεντρωμένοι Αυτόνομοι Οργανισμοί (Decentralized Autonomous Organizations/ DAOs).

---

input, έστω και μικρή, οδηγεί σε διαφορετικό hash value, ενώ η γνώση του hash value δεν μπορεί να οδηγήσει σε αποκρυπτογράφηση του input. (Βλ. Panel for the Future of Science and Technology (STOA) (2019) *Blockchain and the General Data Protection Regulation Can distributed ledgers be squared with European data protection law?* Βρυξέλλες: Ευρωπαϊκό Κοινοβούλιο. Διαθέσιμο στο: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf, σ. 3).

[102] Κάθε block συνδέεται αναπόσπαστα με το προηγούμενό του, ώστε να υπάρχει μια αδιάκοπη αλληλουχία μεταξύ τους. Αυτό συμβαίνει, διότι κάθε block περιλαμβάνει, εκτός από το δικό του ψηφιακό αποτύπωμα, χρονοσήμανση (timestamp) και το ψηφιακό αποτύπωμα του προηγούμενου block. Ως εκ τούτου, κάθε αλλοίωση/μεταβολή στα δεδομένα ενός block επιφέρει ουσιώδεις αλλαγές σε κάθε επόμενο block της αλυσίδας (βλ. ό.π.).

[103] Ό.π. Όσοι χρήστες/κόμβοι έχουν δικαίωμα υποβολής νέων block στην αλυσίδα, ονομάζονται εξορύχοι (miners) και η διεργασία που πραγματοποιούν εξόρυξη (mining).

[104] Τελικά, προκειμένου ένας επιτιθέμενος να αλλοιώσει/μεταβάλει/καταστρέψει δεδομένα σε ένα block, θα πρέπει να αλλάξει όχι μόνο το συγκεκριμένο block, αλλά και όλα τα επόμενα blocks της αλυσίδας, και επιπλέον, να πράξει τούτο σε όλα τα αποθηκευμένα αντίγραφα της αλυσίδας block από τους ομότιμους χρήστες/κόμβους του δικτύου, πράγμα εξαιρετικά δύσκολο, δαπανηρό και χρονοβόρο.

[105] Ο όρος αναφέρεται σε εφαρμογές λογισμικού, ο πάροχος των οποίων ασκεί κυριαρχικό έλεγχο στην εφαρμογή, τα δεδομένα και το περιεχόμενο που παράγεται εντός της και την είσοδο σε αυτήν, με αποτέλεσμα το ουσιαστικό κόστος της αλλαγής παρόχου να είναι ασύμφορο, οι χρήστες της εφαρμογής να «εγκλωβίζονται» σε αυτήν και οι σχετικοί πάροχοι να συγκεντρώνουν απαράμιλλη εξουσία. Στην Αμερική, οι εφαρμογές των GAFAM (Google, Apple, Facebook, Amazon και Microsoft) χαρακτηρίζονται ευλόγως ως "walled gardens".

[106] Ό.π., Panel for the Future of Science and Technology (STOA) (2019), σ. 4.

Ως κρυπτονομίσματα[107] (πχ. Bitcoin, Ethereum, BNB, Solana κ.ο.κ.) χαρακτηρίζονται τα ψηφιακά περιουσιακά στοιχεία που χρησιμοποιούνται ως άυλα μέσα για την εκτέλεση αποκεντρωμένων ψηφιακών συναλλαγών. Για την έκδοση, κυκλοφορία και ρύθμισή τους δεν μεσολαβεί κάποιος κεντρικός οργανισμός ή αρχή (πχ. τράπεζα ή κράτος), αλλά ένα αποκεντρωμένο δίκτυο ομότιμων χρηστών/κόμβων[108]. Είναι άμεσα μετατρέψιμα σε νόμιμο χρήμα (νόμισμα) στα ανταλλακτήρια κρυπτονομισμάτων (πχ. Binance, Kraken, KuCoin κ.ο.κ.) και επιπλέον, επιτρέπεται να ανταλλαχθούν μεταξύ τους για την ίδια ποσότητα[109] (πχ. 1 Bitcoin για 100 εκατομμύρια satoshi[110], 1 Bitcoin για 1 Bitcoin κ.ο.κ.).

Από την άλλη, τα NFTs[111] είναι μονάδες δεδομένων (data units) που εγγράφονται στο Blockchain[112] και λειτουργούν ως μοναδικά αντικείμενα αποκεντρωμένων ψηφιακών συναλλαγών. Εν αντιθέσει με τα κρυπτονομίσματα, τα NFTs δεν επιδέχονται κλασματικές υποδιαιρέσεις ούτε ανταλλάσσονται μεταξύ τους (non-fungibility), καθώς συνδέονται με ένα διακριτό και μοναδικό ψηφιακό αντικείμενο[113] [114](πχ. ένα μουσικό αρχείο, ένα έργο ζωγραφικής, ένα αξεσουάρ για άβαταρ κ.ά), του οποίου αποδεικνύουν την προέλευση, ιδιοκτησία και αυθεντικότητα[115]. Επίσης, περιέχουν και λειτουργούν εν είδει έξυπνων

[107] Το πρώτο κρυπτονόμισμα που κυκλοφόρησε ήταν το Bitcoin, το οποίο εκδόθηκε το 2009 ως λογισμικό ανοιχτού κώδικα. Μέχρι το Μάρτιο του 2022, είχαν κυκλοφορήσει πάνω από 9.000 άλλα κρυπτονομίσματα (βλ. Wikipedia (2023) *Cryptocurrency*, Διαθέσιμο στο: https://en.wikipedia.org/wiki/Cryptocurrency).

[108] (βλ. ό.π.).

[109] Ό.π., Kalpokas, I. and Kalpokienė, J. (2023), σ. 44-45.

[110] Η μικρότερη υποδιαίρεση του Bitcoin.

[111] Το βάπτισμα του πυρός για την εμφάνιση των NFTs δόθηκε το 2012 με την έκδοση των Colored Coins, που αποτέλεσαν μία μέθοδο επισύναψης μεταδεδομένων στις συναλλαγές μέσω Bitcoin. Το πρώτο NFT, γνωστό ως "Quantum", δημιουργήθηκε από τον Kevin McCoy λίγο αργότερα, το 2014. Ο McCoy ενέγραψε το οικείο ψηφιακό αντικείμενο (ένα ψηφιδωτό οκτάγωνο που αλλάζει χρώμα με τρόπο που υπνωτίζει, δίνοντας την εντύπωση ότι πάλλεται) στο Blockchain Namecoin και το πούλησε στον Anil Dash για τέσσερα δολάρια. Αν και καθυστερημένα, μόλις το 2021, το πρώτο αυτό NFT δημοπρατήθηκε από τον οίκο Sotheby's για πάνω από 1 εκατομμύριο δολάρια. Από το 2017 έως σήμερα, η πλειονότητα των NFTs εγγράφονται στο Ethereum blockchain, δυνάμει του τεχνικού προτύπου ERC-721.

[112] Κοντογεώργου, Π., Συρμακέζη, Ζ., Ζούλοβιτς, Μ. (2022) 'Metaverse: βασικές νομικές προκλήσεις στο νέο εικονικό σύμπαν του web3', *Συνήγορος*, 151/2022, σ. 55.

[113] Παραδείγματα ψηφιακών έργων που έγιναν NFTs: Everydays: the First 5000 Days του Beeple, Bored Apes της Yuga Labs, CryptoPunks της Larva Lubs κ.ά.

[114] Ό.π., Kalpokas, I. and Kalpokienė, J. (2023), σ. 45.

[115] Ό.π., Κοντογεώργου, Π., Συρμακέζη, Ζ., Ζούλοβιτς, Μ. (2022).

συμβολαίων (smart contracts)[116] ενσωματωμένων στο Blockchain και μόνο αν προβλέπεται ρητώς στο εκάστοτε έξυπνο συμβόλαιο, χορηγούν δικαιώματα πνευματικής ιδιοκτησίας επί του ψηφιακού έργου με το οποίο συσχετίζονται στον αγοραστή του NFT[117]. Ο όρος "NFT" έχει καταλήξει να χρησιμοποιείται για να χαρακτηρίσει τόσο την ψηφιακή απόδειξη ιδιοκτησίας του υποκείμενου ψηφιακού έργου (proof-of-ownership), η οποία αποθηκεύεται στο Blockchain εν είδει δεδομένων, όσο και το ίδιο το ψηφιακό έργο, το οποίο συνήθως αποθηκεύεται εκτός της αλυσίδας (off-chain), με την ακριβή θέση αυτού να υποδεικνύεται μέσω ενός υπερσυνδέσμου (URL) στο μητρώο του κρυπτοπαραστατικού[118].

Πέραν τούτων, οι DAOS, οι οποίοι ήδη διαχειρίζονται εικονικές πλατφόρμες (πχ. Decentraland[119], TheSandbox[120], Axie Infinity κ.ά), είναι οργανισμοί που διοικούνται από κοινότητες χρηστών χωρίς κεντρική ηγεσία. Το πρώτον, μέσω έξυπνων συμβολαίων ενσωματωμένων στο Blockchain, τα οποία καθορίζουν υπό μορφή κώδικα και εκτελούν αυτόματα τους βασικούς κανόνες λειτουργίας του οργανισμού. Συμπληρωματικά, μέσω ενός συστήματος διακυβέρνησης το οποίο στηρίζεται στη δημοκρατική λήψη αποφάσεων για τον οργανισμό από όλους τους «μετόχους» (stakeholders), επί τη βάσει υποβαλλόμενων προτάσεων (κάθε stakeholder έχει συγκεκριμένο αριθμό ψήφων, ανάλογα με τα tokens που είχε αγοράσει στο στάδιο χρηματοδότησης του οργανισμού)[121].

Το ιδεατό, ανοιχτό και διαλειτουργικό Metaverse είναι δυνατόν να δημιουργηθεί μόνο χάρη στον αποκεντρωμένο χαρακτήρα του Blockchain και των σχετικών εφαρμογών

---

[116] Τα έξυπνα συμβόλαια είναι προγράμματα υπολογιστή, που προορίζονται να εκτελούν αυτόνομα (self-executing) και αυτόματα τους όρους μιας συμφωνίας, εφόσον διαπιστώσουν, κατόπιν σχετικού ελέγχου, ότι πληρούνται οι απαιτούμενες προϋποθέσεις (κατά τη λογική if - then), χωρίς την ανάγκη συμμετοχής ενδιαμέσων, όπως τραπεζών ή δικηγόρων (βλ. Wikipedia (2023) *Smart contract*. Διαθέσιμο στο: https://en.wikipedia.org/wiki/Smart_contract [Πρόσβαση 5 Μαΐου 2023]).

[117] Αν δεν προβλέπεται ρητώς στο έξυπνο συμβόλαιο, ο αγοραστής του NFT αποκτά κατ' αρχήν ένα περιορισμένο δικαίωμα (μη αποκλειστικής) πρόσβασης και (προσωπικής) χρήσης του ψηφιακού έργου που συνδέεται με το NFT (βλ. ό.π., Κοντογεώργου, Π., Συρμακέζη, Ζ., Ζούλοβιτς, Μ. (2022), σ. 55), ενώ δεν μπορεί να προβεί σε εμπορική χρήση του ψηφιακού έργου, στη δημιουργία αντιγράφων προς μεταπώληση ή παραγώγων αυτού κ.ο.κ. (βλ. ό.π., Kalpokas, I. and Kalpokienė, J. (2023), σ. 47).

[118] Παπαθανασίου, Β. (2022) *Μη εναλλάξιμα κρυπτοπαραστατικά - Non-Fungible Tokens, Νομικά ζητήματα & προτάσεις*. Αθήνα: Νομική Βιβλιοθήκη, σ. 20.

[119] Οι χρήστες της Decentraland αγοράζουν εικονικά οικόπεδα με τη μορφή NFTs, χρησιμοποιώντας ως μέσο πληρωμής το κρυπτονόμισμα MANA, που βασίζεται στο Ethereum Blockchain (βλ. Analysis and Research Team (ART) (2022), σ. 5).

[120] Αντίστοιχα, οι χρήστες της The Sandbox αγοράζουν και πωλούν σε μορφή NFTs ψηφιακά αντικείμενα που οι ίδιοι δημιουργούν.

[121] Ό.π., Citi GPS: Global Perspectives & Solutions (2022), σ. 54-55.

του (cryptos, NFTs, DAOs, DeFi[122], dApps[123] κλπ). Στο Blockchain εκτιμάται, λοιπόν, ότι θα αποθηκευτούν οι οικονομικές συναλλαγές που θα συντελεστούν στο Metaverse[124]. Τα NFTs των χρηστών, τα οποία θα λειτουργούν ως αδιάβλητη και ανεξίτηλη απόδειξη της - συνδεόμενης με αυτά - εικονικής περιουσίας τους, θα αποθηκεύονται στο εικονικό πορτοφόλι τους (crypto wallet)[125] και - ιδεατά - τα σχετικά εικονικά αντικείμενα θα μεταφέρονται απρόσκοπτα μεταξύ όλων των πλατφορμών. Τέλος, οι DAOs αναμένεται να διοικούν σε μεγάλο βαθμό τις αποκεντρωμένες πλατφόρμες του Metaverse.

Οι ως άνω τεχνολογίες, σε συνδυασμό με τα ασύρματα δίκτυα 5ης γενιάς (5G)[126], την Υπολογιστική Νέφους (Cloud Computing), αλλά και Παρυφών (Edge Computing)[127], την 3D αρχιτεκτονική σχεδίαση και την Τεχνολογία Ολογράμματος (Holographic Technology)[128], την Τεχνολογία Ψηφιακών Διδύμων (Digital Twins Technology)[129] και πλήθος Διεπαφών

---

[122] Αποκεντρωμένη Χρηματοδότηση (Decentralized Finance): οικοσύστημα παροχής αποκεντρωμένων χρηματοοικονομικών προϊόντων και υπηρεσιών που βασίζεται σε τεχνολογίες όπως το Blockchain. Στο Metaverse, το DeFi αναμένεται να συνδυαστεί με το Traditional Finance (TradFi) και το Centralized Finance (CeFi) (βλ. ό.π., σ. 9).

[123] Αποκεντρωμένες Εφαρμογές (Decentralized Apps): αποκεντρωμένες εφαρμογές λογισμικού που βασίζονται σε τεχνολογίες όπως το Blockchain. Στο Metaverse, οι dApps θα μπορούν να παρέχουν στους χρήστες μία μεγάλη ποικιλία αποκεντρωμένων προϊόντων, υπηρεσιών και εμπειριών, για τη δημιουργία εικονικών κόσμων που δεν θα ελέγχονται από καμία κεντρική οντότητα (βλ. Anidjar, L.Y., Packin, N.G. and Panezi, A. (2023) 'The Matrix of Privacy: Data Infrastructure in the AI-Powered Metaverse', *SSRN Electronic Journal*. 24 Φεβρουαρίου. Διαθέσιμο στο: https://doi.org/10.2139/ssrn.4363208, σ. 17).

[124] Ό.π., Nextrope (2022), σ. 23.

[125] Meshi, D. (2022) 'The metaverse is money and crypto is king – why you'll be on a blockchain when you're virtual-world hopping', *The Conversation*, 14 Ιανουαρίου. Διαθέσιμο στο: https://theconversation.com/the-metaverse-is-money-and-crypto-is-king-why-youll-be-on-a-blockchain-when-youre-virtual-world-hopping-171659 [Πρόσβαση 12 Μαΐου 2023].

[126] Ό.π., Sebastian, G. (2023), σ. 9.

[127] Ό.π., Lim, W.M. et al. (2022), σ. 3.

[128] Η 3D αρχιτεκτονική σχεδίαση και η Τεχνολογία Ολογράμματος θα συνδυαστούν με τα γραφικά της τεχνολογίας XR για τη ρεαλιστική προσομοίωση του εικονικού κόσμου.

[129] Τεχνολογία δυνάμει της οποίας ένα φυσικό αντικείμενο αναπαρίσταται στον εικονικό κόσμο από ένα εικονικό αντικείμενο, που λειτουργεί ως ψηφιακό δίδυμό του. Το ψηφιακό δίδυμο συγχρονίζεται με το φυσικό αντικείμενο, τροφοδοτούμενο από δεδομένα που, ως επί το πλείστον, συλλέγονται σε πραγματικό χρόνο από την τεχνολογία XR και αναλύονται από την Τεχνητή Νοημοσύνη. Η τεχνολογία αυτή επιτρέπει και τη δημιουργία προβλέψεων, τη βελτιστοποίηση και προσαρμογή του ψηφιακού διδύμου. (Βλ. Wang, Y. *et al.* (2022), σ. 325). Για παράδειγμα, τα άβαταρ είναι τα ψηφιακά δίδυμα των χρηστών που ενσαρκώνουν.

Προγραμματισμού Εφαρμογών (Application Programming Interface/APIs)[130], λογισμικού και υλισμικού, θέτουν ήδη τα θεμέλια για την κατασκευή του Metaverse.

Στις τεχνολογίες αυτές ασφαλώς θα προστεθούν και άλλα τεχνολογικά εργαλεία (πχ. τα ασύρματα δίκτυα επόμενης γενιάς 6G)[131], που συνολικά θα αποτελέσουν sine qua non συνθήκη για την ανάπτυξη και λειτουργία του ιδεατού Metaverse. Ωστόσο, βήματα γίνονται και προς μια πιο σκοτεινή κατεύθυνση· ήδη η εταιρεία νευροτεχνολογίας Neuralink Corporation με ιδρυτή τον Elon Musk και άλλους επτά επιστήμονες και μηχανικούς, διεξάγει πειράματα σε ζώα και σύντομα και σε ανθρώπους, για να αναπτύξει εμφυτεύσιμες διεπαφές εγκεφάλου - μηχανής (Brain-Computer Interfaces/BCI) και να πετύχει την απόλυτη εμβύθιση του χρήστη στο Metaverse[132].

2.3 Ανταγωνιστικά οράματα

Το φιλόδοξο τεχνολογικό εγχείρημα για τη δημιουργία του Metaverse ώθησε δικαιολογημένα στη διαμόρφωση περισσότερων ανταγωνιστικών οραμάτων (competing visions) σχετικά με τη μορφή και το μοντέλο διακυβέρνησής του.

Μετά ταύτα, ορισμένοι αρχιτέκτονες του Metaverse προσβλέπουν στην κατασκευή ενός πλήρως εμβυθιστικού εικονικού περιβάλλοντος, υποστηριζόμενου εξ ολοκλήρου από τεχνολογίες Εικονικής Πραγματικότητας, ενώ άλλοι, αντιθέτως, μεταξύ των οποίων και ο Διευθύνων Σύμβουλος της Niantic, John Hanke, οραματίζονται μια εκδοχή του Metaverse που θα λειτουργεί αποκλειστικά με τεχνολογίες Επαυξημένης Πραγματικότητας[133].

Ωστόσο, το σπουδαιότερο σημείο διαφωνίας μεταξύ των ενδιαφερόμενων πλευρών δεν είναι άλλο από το καθεστώς ελέγχου που θα ασκείται στο Metaverse.

Αφενός, στο συγκεντρωτικό (centralized), ιδιωτικό (privatized) Metaverse, η εικονική πλατφόρμα ως υποδομή, η εικονική ταυτότητα, τα εικονικά αντικείμενα, αλλά και το σύνολο των δεδομένων των χρηστών που θα εξάγονται κατά την είσοδο και πλοήγησή τους στο Metaverse, θα αποθηκεύονται σε κεντρικούς servers μίας μόνο ή λίγων ιδιωτικών εταιρειών, που θα ελέγχουν μονοπωλιακά την πρόσβαση, τα δεδομένα, το δημιουργούμενο

---

[130] Ό.π., Sebastian, G. (2023), σ. 4. Σύνολο πρωτοκόλλων και εργαλείων που επιτρέπουν σε διαφορετικές εφαρμογές λογισμικού να επικοινωνούν και να διαλειτουργούν.

[131] Ό.π., σ. 9.

[132] Ό.π., Di Pietro, R. and Cresci, S. (2021), σ. 283.

[133] Clifford Chance (2022) 'The Metaverse: What are the legal implications?' Διαθέσιμο στο: https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2022/02/the-metaverse-what-are-the-legal-implications.pdf, σ. 2.

περιεχόμενο και την εν γένει δραστηριότητα των χρηστών εντός της πλατφόρμας, μέσω προδιατυπωμένων και επαχθών Όρων Παροχής Υπηρεσιών (Terms of Service/ToS)[134].

Αυτή η δυστοπική εκδοχή του Metaverse θα θυμίζει τη διαδικτυακή εμπειρία εντός των κλειστών πλατφορμών του WEB 2.0, την οποία χαρακτηρίζουν οι πολλαπλές συνδέσεις *("multiple logins")*, η ανάδειξη των οικείων παρόχων ως ρυθμιστών της πρόσβασης στο Διαδίκτυο *("platform gatekeepers")*, η εμπορευματοποίηση των προσωπικών δεδομένων των χρηστών *("user data monetization")* και η ενσωματωμένη διαφήμιση *("embedded advertising")*[135]· επιπλέον, η έλλειψη επαρκούς ανταμοιβής των χρηστών για το δημιουργούμενο ψηφιακό περιεχόμενο, συνδυαστικά με την αδυναμία εξαργύρωσης ή μεταφοράς της αξίας αυτού εκτός της πλατφόρμας *("limited financial inclusion")*, αλλά και ο κίνδυνος απομείωσης της αξίας του, απαγόρευσης της πρόσβασης σε αυτό, κατάσχεσης ή διαγραφής του *("de-monetization")* ή αυθαίρετου αποκλεισμού του χρήστη από την πλατφόρμα *("de-platforming")*, λόγω μονομερούς μεταβολής των σχετικών Όρων Παροχής Υπηρεσιών από τον πάροχο[136]. Συνεπώς, το Metaverse που θα υιοθετήσει αυτά τα χαρακτηριστικά θα είναι ένα κλειστό (closed), βασισμένο στο WEB 2.0 (WEB2-based) Metaverse[137], με τη μόνη διαφορά ότι θα παρέχει τη δυνατότητα ρεαλιστικής εμβύθισης στους χρήστες[138].

Αφετέρου, στο αποκεντρωμένο (decentralized), κοινόχρηστο (communal) Metaverse, όλα τα παραπάνω (i.e., η πλατφόρμα, η ταυτότητα, τα αντικείμενα και τα δεδομένα) θα αποθηκεύονται σε αποκεντρωμένα δίκτυα υπολογιστών - κόμβων, που θα λειτουργούν επί τη βάσει αποκεντρωμένων τεχνολογιών όπως το Blockchain, παρέχοντας στους χρήστες του εικονικού κόσμου κυριαρχικό έλεγχο και δικαιώματα ιδιοκτησίας επί των δεδομένων τους και επί του εικονικού περιεχομένου που δημιουργούν ή αποκτούν *("sovereign ownership of data")*[139], φορητότητα των δεδομένων και διαλειτουργικότητα μεταξύ των πλατφορμών *("portability of data, and interoperability between platforms")*[140].

---

[134] Συναντώνται και ως Όροι Χρήσης (Terms of Use/ToU) ή Όροι και Προϋποθέσεις (Terms and Conditions/T&C). Πρόκειται για τις νομικές συμφωνίες μεταξύ του παρόχου μιας υπηρεσίας και του τελικού χρήστη που θέλει να τη χρησιμοποιήσει.

[135] Ό.π., Citi GPS: Global Perspectives & Solutions (2022), σ. 47.

[136] Ό.π., σ. 57.

[137] Ό.π., σ. 47.

[138] Ό.π., σ. 26.

[139] Ό.π.

[140] Ό.π.

Στην ουτοπική εκδοχή του Metaverse, διάφορες κοινότητες χρηστών θα χτίζουν και θα κυβερνούν το δικό τους εικονικό σύμπαν[141] με αποκεντρωμένο και δημοκρατικό τρόπο, αποτρέποντας την ανάπτυξη μονοπωλίων (βλ. το παράδειγμα των DAOs). Την ίδια στιγμή, οι χρήστες θα εισέρχονται και θα μετακινούνται μεταξύ των διάφορων αποκεντρωμένων πλατφορμών ελεύθερα, συνδεόμενοι σε έκαστη από αυτές με ένα απλό κλικ στο εικονικό τους πορτοφόλι *("login-free and password-free movement between virtual worlds driven by wallet-enabled, one-click sign-in")*[142]. Αυτό θα εμπεριέχει το σύνολο των προσωπικών λογαριασμών και φιλικών επαφών τους, αλλά και της εικονικής περιουσίας τους (πχ. άβαταρ, ενδυμασίες - skins, αξεσουάρ, εικονικά ακίνητα κ.ά.) υπό μορφή NFTs και θα υποστηρίζει την αποκεντρωμένη ταυτοποίηση των χρηστών (decentralized authentication), επιτρέποντάς τους να αποφασίσουν αυτόνομα ποια από όλα τα ανωτέρω επιθυμούν να αποκαλύψουν ή να μεταφέρουν σε κάθε πλατφόρμα *("…would allow the user to selectively expose their identity and property for different use cases as they deem fit, with full self-sovereignty… without handing over all of the player's data to the platform")*[143]. Θα πρόκειται, λοιπόν, για ένα ανοιχτό (open), βασισμένο στο WEB 3.0 (WEB3-based) Metaverse[144], στο οποίο η δύναμη θα μετατοπιστεί από τους μεγάλους παρόχους του WEB 2.0 στους ίδιους τους χρήστες του εικονικού κόσμου.

Μια τρίτη εκδοχή είναι η επικράτηση υβριδικών σχημάτων (hybrid Metaverse)[145], που θα υιοθετούν χαρακτηριστικά των δύο προηγούμενων. Εν προκειμένω, ιδιωτικές εταιρείες θα κατακλύσουν τη σχετική αγορά, κατασκευάζοντας και προσφέροντας την αναγκαία υποδομή για το Metaverse. Παράλληλα όμως, θα αξιοποιούν αποκεντρωμένες τεχνολογίες, όπως το Blockchain, με σκοπό την εγκαθίδρυση ενός πιο ανοιχτού, διαλειτουργικού και

[141] Ό.π., European Parliamentary Research Service (EPRS) (2022), σ. 2.
[142] Ό.π., σελ. 52.
[143] Ό.π., σελ. 52.
[144] Ό.π., σ. 47.
[145] Ό.π., σ. 27.

συμμετοχικού περιβάλλοντος[146], εντός του οποίου - όπως υποστηρίζουν - οι τελικοί χρήστες θα ασκούν ουσιαστικό έλεγχο επί της εικονικής τους περιουσίας[147].

Εντούτοις, τέτοιου είδους εξαγγελίες πρέπει να αντιμετωπίζονται - το λιγότερο - με επιφύλαξη. Ο ακριβής καθορισμός των δικαιωμάτων ιδιοκτησίας που θα χορηγούνται στους χρήστες επί του εικονικού αγαθού που αποκτούν υπό μορφή NFT, θα ρυθμίζεται σε πρώτη φάση από το οικείο έξυπνο συμβόλαιο[148], ενώ ακόμη κι αν τέτοια δικαιώματα πράγματι προσποριζονται στους χρήστες, η τύχη του ψηφιακού έργου που συνδέεται με το NFT (αν θα τίθεται ως έχει στη διάθεση του χρήστη ή θα τροποποιείται, διαγράφεται, αποσυνδέεται από την εγγραφή στο Blockchain κ.ο.κ.) θα ρυθμίζεται τελικά από τους μονομερώς επιβαλλόμενους και αυθαίρετα μεταβαλλόμενους Όρους Παροχής Υπηρεσιών των παρόχων[149]. Εξάλλου, όπως προβλέπεται, οι συμμετέχουσες εταιρείες θα υιοθετήσουν διαλειτουργικά πρότυπα μόνο σχετικά με το χρησιμοποιούμενο υλισμικό που θα παρέχει την πρόσβαση στο Metaverse και όχι σχετικά με το συναφές λογισμικό[150] ή την χρησιμοποιούμενη από την πλατφόρμα αλυσίδα Blockchain, με αποτέλεσμα η αξία των εικονικών αγαθών που οι χρήστες θα κατέχουν μέσω NFTs να αναλώνεται τελικά εντός των στενών συνόρων της εκάστοτε ιδιωτικής πλατφόρμας.

Επιπλέον, ενώ το Metaverse φημολογείται ενίοτε ότι θα είναι μία ενιαία οντότητα που θα παρέχεται μέσω μίας μοναδικής πλατφόρμας (singular, unitary Metaverse), άλλοι το αντιλαμβάνονται ορθά ως "metaverses", δηλαδή ως διακριτά εικονικά οικοσυστήματα, που θα ανήκουν σε διαφορετικούς ιδιοκτήτες και δεν θα συνδέονται απαραίτητα μεταξύ τους[151]. Μεταξύ των οπαδών της τελευταίας εκδοχής, ο Διευθύνων Σύμβουλος της The Walt Disney Company, Bob Chapek, φιλοδοξεί να αναπτύξει ένα διακριτό "Disney Metaverse"[152]. Η Meta Platforms παραδέχεται, πάντως, ότι «*το metaverse δεν είναι ένα μοναδικό προϊόν το οποίο*

[146] Βλ. διάκριση μεταξύ ενός "*centralized blockchain-based metaverse*", ενός "*more centralized metaverse*" και ενός "*decentralized blockchain-based metaverse*", Knibbeler, D., Mohrmann, M. and Zadeh, S. (2022) 'EU: Privacy and security concerns in the metaverse', Αύγουστος 2022. Διαθέσιμο στο: https://www.dataguidance.com/opinion/eu-privacy-and-security-concerns-metaverse [Πρόσβαση 12 Μαΐου 2023].

[147] Mangada Real de Asúa, E. et al. (2022) 'The Metaverse: Challenges and regulatory issues', *SciencesPo*. Διαθέσιμο στο: https://www.sciencespo.fr/public/sites/sciencespo.fr.public/files/Metaverse-Group-report-final-draft-June-12-1.pdf, σ. 20.

[148] Ό.π., Kalpokas, I. and Kalpokienė, J. (2023), σ. 46.

[149] Ό.π., σ. 47.

[150] Ό.π., σ. 36.

[151] Ό.π., Clifford Chance (2022), σ. 2.

[152] Ό.π., σ. 2.

μπορεί μια εταιρεία να χτίσει μόνη. Ακριβώς όπως το διαδίκτυο, το metaverse υπάρχει είτε το Facebook είναι εκεί είτε όχι»[153]. Επί της ουσίας, το Metaverse, όπως το Διαδίκτυο, θα είναι μοναδικό και δεν θα ελέγχεται από κανέναν[154], απλώς η είσοδος σε αυτό θα διευκολύνεται ή και ελέγχεται από πλήθος διαφορετικών παρόχων.

Τέλος, παρατηρείται μια δυναμική, γεωπολιτικής φύσεως συσπείρωση μεταξύ των ενδιαφερόμενων χωρών. Χαρακτηριστικά, η Νότια Κορέα έχει αναγγείλει την "Metaverse Alliance"[155]· η κομμουνιστική Κίνα έχει δημιουργήσει την "Metaverse Industry Committee", ενώ είναι πολύ πιθανό να αρχίσει να ανταγωνίζεται τη Δύση και ιδίως τις ΗΠΑ, οι οποίες πρωτοστατούν στην κούρσα για την επικράτηση στο Metaverse[156]· η Ευρώπη, από την άλλη, παρότι τεχνολογικά ανίσχυρη συγκριτικά, εξάγει ρυθμιστική τεχνογνωσία, γεγονός που ενδέχεται να την καταστήσει σημαντικό παίκτη της οικείας αγοράς.

Η δομή του Metaverse συνιστά μήλο της έριδος για τους διάφορους εμπλεκόμενους φορείς, καθένας εκ των οποίων υπηρετεί διαφορετικά, αν όχι αντικρουόμενα συμφέροντα. Κατά τη γνώμη της γράφουσας, τουλάχιστον στην αυγή της δημιουργίας του, το Metaverse θα χαρακτηρίζεται από ένα ετερόκλητο μείγμα συμμετεχόντων, ενώ συν τω χρόνω, οι υβριδικές πλατφόρμες εικονικής πραγματικότητας θα λάβουν τη μερίδα του λέοντος στην οικεία αγορά και, παράλληλα με τις γεωπολιτικές αντιπαλότητες, θα οδηγήσουν στην κατάτμηση του εικονικού χώρου. Ευλόγως, η αρχιτεκτονική του Metaverse θα αποτελέσει καθοριστικό παράγοντα για την ευρεία ή περιορισμένη απήχησή του στην ψηφιακή αγορά.

3. ΤΟ METAVERSE ΩΣ ΝΕΑ ΕΠΕΝΔΥΤΙΚΗ ΤΑΣΗ

Ο κύριος στόχος των παρόχων των πλατφορμών Metaverse είναι να δημιουργήσουν ολοκληρωμένους κόσμους, στους οποίους οι χρήστες θα μπορούν να ζήσουν εικονικά κάθε πτυχή της καθημερινότητάς τους *("all-encompassing")*[157]. Υπό αυτή την έννοια, το Metaverse αναμένεται να φέρει την επανάσταση στους περισσότερους - αν όχι σε όλους - τους τομείς

---

[153] Bosworth, A. and Clegg, N. (2021) 'Building the Metaverse Responsibly', *Meta*, 27 Σεπτεμβρίου. Διαθέσιμο στο: https://about.fb.com/news/2021/09/building-the-metaverse-responsibly/ [Πρόσβαση 12 Μαΐου 2023].

[154] Κουσουνή-Πανταζοπούλου, Α. (2023), ό.π., σ. 378.

[155] Kim, S. (2021) 'South Korea's Approach to the Metaverse', *The Diplomat*, 2 Νοεμβρίου. Διαθέσιμο στο: https://thediplomat.com/2021/11/south-koreas-approach-to-the-metaverse/ [Πρόσβαση 12 Μαΐου 2023].

[156] Ό.π., Analysis and Research Team (ART) (2022), σ. 9.

[157] Ό.π., Kalpokas, I. and Kalpokienė, J. (2023), σ. 53.

της ανθρώπινης δραστηριότητας και κατ' επέκταση να δημιουργήσει άπειρες ευκαιρίες για κερδοφορία στους συμμετέχοντες.

Μετά ταύτα, η προσπάθεια για τη δημιουργία του και την έγκαιρη εγκατάσταση σε αυτό έχει εξελιχθεί σε αγώνα δρόμου, στον οποίο συμμετέχουν, έστω από φόβο μην μείνουν πίσω[158], κορυφαίες, αναπτυσσόμενες και νεοφυείς (start-ups) επιχειρήσεις από διάφορους τομείς[159], κοινότητες χρηστών με αποκεντρωμένη διοίκηση (βλ. DAOs), διασημότητες από τη βιομηχανία του θεάματος και τον καλλιτεχνικό χώρο, αλλά και κρατικές οντότητες. Η PwC εκτιμά ότι η συνολική αξία της τροφοδοτούμενης από το Metaverse αγοράς θα έχει εκτιναχθεί στα 1,5 τρισεκατομμύρια δολάρια έως τα τέλη του 2030[160], ενώ ακόμη και πιο συγκρατημένες φωνές κάνουν λόγο για μια αγορά 8-13 δισεκατομμυρίων έως τότε[161]! Ενδεικτικά, το Metaverse *υπόσχεται* να ενισχύσει και μεταρρυθμίσει τους κάτωθι τομείς:

1. Το εμπόριο και εν γένει τις οικονομικές συναλλαγές: Στο εικονικό περιβάλλον του Metaverse θα δραστηριοποιηθούν επιχειρήσεις και εταιρείες του πραγματικού κόσμου, με σκοπό να αυξήσουν την αξία και τη φήμη του εμπορικού τους σήματος εκτός Metaverse ή και να προωθήσουν B2B / B2C προϊόντα / υπηρεσίες που θα υπηρετούν αποκλειστικά το Metaverse οικοσύστημα[162]. Για παράδειγμα, η Nike ήδη συνεργάστηκε με την Epic Games για τη δημιουργία μιας εικονικής συλλογής Air Jordan, που θα μπορεί να φορεθεί από τα άβαταρ στο εικονικό παιχνίδι Fortnite[163]. Επίσης, θα γεννηθεί το λεγόμενο "metabranding",

---

[158] Κατά το σύνδρομο FoMO, που αποτελεί ακρωνύμιο για το "Fear of Missing Out".

[159] Γενικά, πάροχοι πλατφορμών κοινωνικών δικτύων, διαδικτυακών παιχνιδιών και ηλεκτρονικού εμπορίου, υπηρεσιών νέφους και χρηματοοικονομικών υπηρεσιών, κατασκευαστές λογισμικού, υλισμικού, δημοφιλή brands κ.ά. Ειδικά, πρωτοπόροι στο εγχείρημα έχουν αναδειχτεί τεχνολογικοί κολοσσοί, όπως οι αμερικανικές Meta Platforms, Microsoft, Alphabet (Google), Nvidia, Qualcomm, οι κινεζικές Alibaba Group και ByteDance, η ιαπωνική Sony κ.ά., αλλά και σημαντικοί παίκτες της βιομηχανίας διαδικτυακών παιχνιδιών, όπως οι αμερικανικές Epic Games (Fortnite), Roblox Corporation (Roblox), Niantic (Pokémon Go), Linden Lab (Second Life), Unity Technologies, η κινεζική Tencent κ.ά. Παρομοίως, παγκοσμίου φήμης brands, πχ. οι αμερικανές Nike, McDonald's, η ιταλική Gucci, η γαλλική Hermès, η γερμανική BMW, η ισπανική FC Barcelona κ.ά., έχουν ήδη πραγματοποιήσει επιχειρηματικές κινήσεις για την είσοδό τους στο χώρο.

[160] GSMA Intelligence (2022) 'Exploring the metaverse and the digital future'. Διαθέσιμο στο: https://www.gsma.com/asia-pacific/wp-content/uploads/2022/02/270222-Exploring-the-metaverse-and-the-digital-future.pdf, σ. 9.

[161] Ό.π., Citi GPS: Global Perspectives & Solutions (2022), σ. 3.

[162] Ό.π., Mangada Real de Asúa, E. et al. (2022), σ. 7.

[163] Ό.π., Clifford Chance (2022), σ. 3.

δηλαδή θα αναδυθούν brands με αποκλειστική παρουσία και δραστηριότητα στο χώρο του Metaverse[164].

Αντίστοιχα, οι χρήστες – καταναλωτές θα έχουν τη δυνατότητα να περιηγούνται σε εικονικά εμπορικά καταστήματα (virtual stores) ή πολυκαταστήματα (virtual malls) με 3D δοκιμαστήρια[165]· να αλληλεπιδρούν με άλλους χρήστες ή bots που θα προσφέρουν υπηρεσίες εξυπηρέτησης πελατών (virtual assistants), διαφήμισης (virtual influencers) ή θα παρίστανται ως εικονικοί αντιπρόσωποι (virtual representatives) των εμπορικών σημάτων στο Metaverse[166]· να παραγγέλνουν προϊόντα που θα παραδίδονται στην πόρτα του (αληθινού) σπιτιού τους[167]· να προμηθεύονται ενδύματα, υποδήματα και αξεσουάρ (virtual fashion)[168] με τη μορφή NFTs από σχετικές αγορές (marketplaces) για να κοσμήσουν τα άβατάρ τους· να επενδύουν σε ψηφιακά ακίνητα (virtual real estate), ψηφιακά έργα τέχνης (virtual art) και συλλεκτικά αντικείμενα (collectibles) που θα πωλούνται ως NFTs για να στεγάσουν και διακοσμήσουν την εικονική κατοικία τους[169]· να συμμετέχουν σε εικονικά καλλιτεχνικά και αθλητικά δρώμενα, αγοράζοντας εισιτήρια επίσης υπό μορφή NFTs για να σφυρηλατήσουν κοινωνικούς δεσμούς κ.ο.κ. Πολλώ δε μάλλον, το Metaverse θα καθιερώσει μια νέα γενιά καταναλωτών, οι οποίοι θα μπορούν όχι μόνο να καταναλώνουν αξία (consumers), αλλά συγχρόνως να παράγουν οι ίδιοι αξία (producers), για την οποία μάλιστα θα αμείβονται, δημιουργώντας και προσφέροντας εικονικές εμπειρίες, αγαθά και υπηρεσίες στο Metaverse κοινό[170]. Η Gen Z θα είναι από τις πρώτες γενιές, λοιπόν, που θα ανήκει στους λεγόμενους "prosumers"του Metaverse.

Όλες οι ανωτέρω επιλογές μεταφράζονται σε απαράμιλλη οικονομική αξία για τους συμμετέχοντες. Αρκεί να σκεφτεί κανείς για να πειστεί, την περίπτωση ενός χρήστη του The Sandbox που αγόρασε πρόσφατα ένα ψηφιακό οικόπεδο εντός της πλατφόρμας αντί 400 περίπου χιλιάδων ευρώ, προσβλέποντας να γίνει ο εικονικός γείτονας του διάσημου τραγουδιστή Snoop Dog[171], ή την επιχειρηματική κίνηση της εταιρείας Republic Realm που

[164] Ό.π.

[165] Ό.π., Kevins, J. (2022), σ. 6.

[166] Ό.π., Citi GPS: Global Perspectives & Solutions (2022), σ. 31.

[167] Ό.π., Kalpokas, I. and Kalpokienė, J. (2023), σ. 57.

[168] Ό.π.

[169] Ό.π., Kevins, J. (2022).

[170] Ό.π., Kalpokas, I. and Kalpokienė, J. (2023), σ. 54.

[171] Ό.π., European Parliamentary Research Service (EPRS) (2022), σ. 3.

επένδυσε ποσό - ρεκόρ - ύψους 4,3 εκατομμυρίων δολαρίων σε αγορά εικονικού ακινήτου για να αναπτυχθεί στην ίδια πλατφόρμα[172].

2. Τις τέχνες και την ψυχαγωγία: Το πεδίο αυτό θα αλλάξει ριζικά με την ανάπτυξη του Metaverse. Εκεί θα διοργανώνονται ποικίλες εικονικές εκδηλώσεις (virtual events), τις οποίες οι χρήστες θα μπορούν να παρακολουθήσουν ενεργά ως άβαταρ από οπουδήποτε στον κόσμο. Τα παρακάτω παραδείγματα προσφέρουν μία πρόγευση των ευκαιριών που αναμένεται να γεννηθούν: οι συναυλίες των δημοφιλών τραγουδιστών Travis Scott και Ariana Grande στο Fortnite συγκέντρωσαν εν μέσω πανδημίας εκατομμύρια θεατές[173], ενώ λόγω αυτών των εξελίξεων, το MTV προσέθεσε την κατηγορία «Καλύτερη Metaverse Ερμηνεία» στα Video Music Awards· τον Μάρτιο του 2022, η Decentraland φιλοξένησε την εικονική «Metaverse Εβδομάδα Μόδας»[174]· στο Παγκόσμιο Κύπελλο Ποδοσφαίρου της FIFA που διεξήχθη στο Κατάρ το 2022, οι θεατές είχαν την επιλογή να παρακολουθήσουν live το παιχνίδι κατεβάζοντας στο κινητό τους μία ειδική εφαρμογή AR, η οποία προσέφερε λεπτομερή στατιστικά στοιχεία για τον αγώνα, τους παίκτες, τις αντίπαλες ομάδες και γενικά τη διοργάνωση καθ' όλη τη διάρκεια του παιχνιδιού[175]· η Pixlr Genesis στοχεύει να χτίσει το «Λούβρο του Metaverse», το μεγαλύτερο αποκεντρωμένο μουσείο τέχνης στο Metaverse, όπου τα έργα θα εκτίθενται υπό μορφή NFTs[176]. Επιπλέον, οι δισκογραφικές και κινηματογραφικές εταιρείες παραγωγής θα μπορούν να χτίζουν συνεργασίες με παρόχους υπηρεσιών Metaverse για την εικονική ή hybrid προβολή μουσικού και οπτικοακουστικού περιεχομένου[177]. Η βιομηχανία gaming, επίσης, θα ανθίσει στο Metaverse. Η χρήση XR εργαλείων για την παροχή εμβυθιστικών εμπειριών παιχνιδιού, αλλά και η προώθηση play-to-earn οικονομικών μοντέλων σε συνδυασμό με το Blockchain, όπου οι χρήστες θα κερδίζουν βραβεία υπό μορφή κρυπτονομισμάτων και NFTs όσο παίζουν, θα ωθήσει στην εκθετική αύξηση της κοινότητας χρηστών των διαδικτυακών παιχνιδιών[178].

---

[172] Αγοράζοντας 792 NFTs, η εταιρεία απέκτησε εικονική έκταση 1.200 οικοδομικών τετραγώνων (βλ. Marinotti, J. (2022) 'Can you truly own anything in the metaverse? A law professor explains how blockchains and NFTs don't protect virtual property', *The Conversation*, 21 Απριλίου. Διαθέσιμο στο: https://theconversation.com/can-you-truly-own-anything-in-the-metaverse-a-law-professor-explains-how-blockchains-and-nfts-dont-protect-virtual-property-179067) [Πρόσβαση 12 Μαΐου 2023].

[173] Ό.π., Kevins, J. (2022), σ. 7.

[174] Ό.π., Clifford Chance (2022), σ. 3.

[175] Ό.π., Aamir, O. (2022), σ. 12-13.

[176] Ό.π., Citi GPS: Global Perspectives & Solutions (2022), σ. 30.

[177] Ό.π., Kalpokas, I. and Kalpokienė, J. (2023), σ. 62.

[178] Ό.π., Citi GPS: Global Perspectives & Solutions (2022), σ. 35-36.

3. Την εργασία: Ένας από τους πρωταρχικούς λόγους για τον οποίο οι άνθρωποι θα εισέρχονται στο Metaverse θα είναι για να εργασθούν. Η εξ αποστάσεως εργασία καθιερώθηκε μεν ευρέως κατά τη διάρκεια της πανδημίας, ωστόσο δεν μπορεί να ανταγωνιστεί το πλεονέκτημα της παραδοσιακής μορφής εργασίας που δεν είναι άλλο από τη φυσική επαφή και επικοινωνία μεταξύ των ανθρώπων. Στο Metaverse οι ισορροπίες αυτές θα αλλάξουν και τα 3D διαδικτυακά meetings θα γεφυρώνουν την απόσταση των τηλεργαζομένων. Προς το σκοπό αυτό, η Meta Platforms επενδύει στην πλατφόρμα Horizon Workrooms, ενώ η Microsoft στην αντίστοιχη πλατφόρμα Mesh[179]. Ταυτόχρονα, εργοδότες ή το αρμόδιο Τμήμα Ανθρώπινου Δυναμικού (Human Resources/HR) θα προσλαμβάνουν προσωπικό κατόπιν αναζήτησης και σύνδεσης με νέα ταλέντα στο Metaverse[180]. Αργότερα, θα εκπαιδεύουν το νεοπροσληφθέν προσωπικό με πιο δημιουργικό και αποτελεσματικό τρόπο[181]. Η Samsung Electronics έχει ήδη επιδιώξει να προσλάβει υπαλλήλους μέσω της εικονικής πλατφόρμας Gather Town[182]. Περαιτέρω, το Metaverse θα επιτρέψει σε υποαμειβόμενους εργαζομένους να αναζητήσουν εργασιακές ευκαιρίες σε χώρες με υψηλότερο εισόδημα και σε κάθε περίπτωση, θα διασφαλίσει ένα πιο ελεύθερο και ευέλικτο εργασιακό καθεστώς[183].

4. Την εκπαίδευση: Το Metaverse αναμένεται να αποτελέσει σημαντικό εργαλείο για εκπαιδευτικούς σκοπούς[184]. Μέσω 3D εμβυθιστικών αναπαραστάσεων, οι καθηγητές θα μπορούν να κεντρίσουν το ενδιαφέρον των φοιτητών τους, αλλά και να προσεγγίσουν δυσνόητες φιλοσοφικές έννοιες, να εξηγήσουν ιστορικά σημεία και να επιλύσουν σύνθετα προβλήματα των θετικών επιστημών με πιο κατανοητό τρόπο. Επομένως, τα εκπαιδευτικά ιδρύματα που θα επενδύσουν περισσότερο στο Metaverse, θα προσελκύσουν και τους πιο φιλόδοξους και ταλαντούχους φοιτητές[185]. Περαιτέρω, ακόμη και ο στρατός των ΗΠΑ έχει αρχίσει να εξερευνά τις δυνατότητες του Metaverse για την αποτελεσματική εκπαίδευση των ενόπλων δυνάμεων[186]. Οπωσδήποτε, η βιωματική εκπαίδευση που αυτό θα παρέχει, θα καταστεί το κλειδί για μια βαθύτερη και πληρέστερη γνώση σε πλήθος τομέων.

---

[179] Ό.π.

[180] Ό.π., σ. 34.

[181] Ό.π.

[182] Ό.π.

[183] Ό.π., Kalpokas, I. and Kalpokienė, J. (2023), σ. 56.

[184] Ό.π., Mangada Real de Asúa, E. et al. (2022), σ. 13.

[185] Ό.π., Kalpokas, I. and Kalpokienė, J. (2023), σ. 60.

[186] Ό.π., European Parliamentary Research Service (EPRS) (2022), σ. 3.

5. Την ιατρική επιστήμη και την υγεία: Ομοίως, το Metaverse δύναται να ενισχύσει ουσιωδώς τους τομείς της ιατρικής και της υγείας. Στον μακρύ κατάλογο των δυνατοτήτων που προσφέρονται, περιλαμβάνονται προσομοιώσεις χειρουργικών επεμβάσεων με σκοπό την πρακτική εξάσκηση των νέων επαγγελματιών, η τηλεχειρουργική, εφαρμογές VR για τη διαχείριση του μετατραυματικού άγχους κ.ο.κ[187]. Το 2021, η Ασιατική Εταιρεία Καρδιαγγειακής και Θωρακικής Χειρουργικής (ASCVTS) εκπαίδευσε 200 θωρακοχειρουργούς στη χειρουργική του καρκίνου του πνεύμονα μέσω μιας πλατφόρμας τύπου Metaverse σε ένα διαδικτυακό συνέδριο[188].

6. Τις έξυπνες πόλεις (smart cities) και τον τουρισμό: Η υλοποίηση του Metaverse θα σημάνει την ανέγερση έξυπνων πόλεων. Στη Νότια Κορέα, η Σεούλ ανακοίνωσε ότι θα είναι η πρώτη πόλη στον κόσμο που θα εισέλθει στο χώρο του Metaverse εντός του 2023, με τη δημιουργία εικονικών σημείων εξυπηρέτησης, όπου οι πολίτες της Σεούλ θα μπορούν εύκολα να διεκπεραιώνουν γραφειοκρατικές υποθέσεις, συναλλασσόμενοι με υπαλλήλους - άβαταρ[189]. Από την άλλη, τα νησιά Barbados προσβλέπουν στη δημιουργία μιας πρεσβείας στο Metaverse, ενώ η πόλη Santa Monica της California έχει προτείνει την εφαρμογή τεχνολογιών Επαυξημένης Πραγματικότητας σε ολόκληρη την πόλη, ώστε οι πολίτες να αισθάνονται ότι βρίσκονται συνεχώς σε βιντεοπαιχνίδι[190]. Ασφαλώς, η δημιουργία έξυπνων πόλεων στοχεύει παράλληλα και στην ενίσχυση του τουρισμού, καθιστώντας τον αστικό ιστό πόλο έλξης για τους ξένους επισκέπτες. Εκτός αυτού, σε μια εποχή όπου η ταξιδιωτική βιομηχανία λιθοβολείται τακτικά για τις αρνητικές περιβαλλοντικές επιπτώσεις της, η εικονική αναπαράσταση τουριστικών χώρων και μνημείων και η επίσκεψη αυτών χωρίς πραγματική μετακίνηση παρίσταται ως μια πιο ελκυστική και ηθική επιλογή[191].

Συμπερασματικά, οι πρακτικές εφαρμογές και τα οφέλη που θα προκύψουν για την κοινωνία και την παγκόσμια αγορά από την υλοποίηση του Metaverse είναι, αν μη τι άλλο, απεριόριστα, ενώ εκτείνονται σε όλους τους τομείς της καθημερινής ζωής, δημιουργώντας εύλογα μια - δίχως προηγούμενο -επενδυτική τρέλα.

4. Η ΕΥΡΩΠΑΙΚΗ ΑΝΤΖΕΝΤΑ ΓΙΑ ΤΟ METAVERSE

[187] Ό.π., Clifford Chance (2022), σ. 3.

[188] Ό.π., Citi GPS: Global Perspectives & Solutions (2022), σ. 33.

[189] Ό.π., European Parliamentary Research Service (EPRS) (2022).

[190] Ό.π., Mangada Real de Asúa, E. et al. (2022), σ. 9.

[191] Ό.π., Kalpokas, I. and Kalpokienė, J. (2023), σ. 62.

Οι εξαγγελίες για την έλευση του Metaverse έχουν ήδη απασχολήσει τα αρμόδια ευρωπαϊκά όργανα σε σχέση με το εφαρμοστέο καθεστώς που πρόκειται να το ρυθμίσει.

Η Πρόεδρος της Ευρωπαϊκής Επιτροπής, Ursula Gertrud von der Leyen, ανακοίνωσε με επιστολή της στις 14 Σεπτεμβρίου 2022 ότι η Ευρωπαϊκή Επιτροπή θα θέσει σε εφαρμογή μια *«Πρωτοβουλία για εικονικούς κόσμους, όπως το metaverse» (Initiative on virtual worlds, such as metaverse)* εντός του 2023, αναγγέλλοντας έτσι τη δέσμευση του θεσμικού αυτού οργάνου της ΕΕ να θέσει σύντομα επί τάπητος καίρια ρυθμιστικά ζητήματα για το Metaverse.

Παράλληλα, ο Ευρωπαίος Επίτροπος για την εσωτερική αγορά, Thierry Breton, σε σχετική ανακοίνωσή του της ίδιας ημέρας, παρομοίασε το Metaverse με την Αρχαία Αγορά των Ελλήνων, επισημαίνοντας πως αυτό, ως *δημόσιος* χώρος, θα πρέπει να διαπνέεται εξ αρχής από τις ευρωπαϊκές αξίες και να δημιουργεί αίσθημα ασφάλειας στους Ευρωπαίους πολίτες. Ως εκ τούτου, τόνισε, θα πρέπει να ρυθμίζεται από διαλειτουργικά πρότυπα και επουδενί από μονομερώς επιβεβλημένους όρους ιδιωτών παικτών εις βάρος της καινοτομίας και του ελεύθερου ανταγωνισμού[192].

Στο πλαίσιο αυτό, εγκαινίασε την πλατφόρμα "Virtual and Augmented Reality Industrial Coalition", που θα αποτελέσει έναν δίαυλο εποικοδομητικού διαλόγου μεταξύ των ενδιαφερομένων μερών για το Metaverse, με στόχο τη διευκόλυνση της κοινής χάραξης πολιτικής, την ενθάρρυνση των επενδύσεων, τον εντοπισμό των βασικών προκλήσεων στον ευρωπαϊκό τομέα VR/AR κ.ο.κ[193]. Εξάλλου, όπως υπογράμμισε, οι Κανονισμοί για τις Ψηφιακές Υπηρεσίες (διεθνώς Digital Services Act/DSA, εφεξής «Κανονισμός DSA») και τις Ψηφιακές Αγορές (διεθνώς Digital Markets Act/DMA) αποτελούν ισχυρά εργαλεία στο οπλοστάσιο της ΕΕ για τον ψηφιακό χώρο.

Σε κάθε περίπτωση, είναι σκόπιμο να μελετηθεί από την ΕΕ αν το ισχύον ενωσιακό νομοθετικό πλαίσιο το οποίο εφαρμόζεται στον ψηφιακό κόσμο, αναμένεται να ρυθμίσει mutatis mutandis και το εικονικό περιβάλλον του Metaverse.

Άραγε ποιες νομικές προκλήσεις είναι πιθανό να προκύψουν κατά την εφαρμογή των ισχυόντων κανόνων ενωσιακού δικαίου στο Metaverse; Θα κριθεί τελικά ως ασφαλές και ικανοποιητικό το επίπεδο προστασίας της ενωσιακής νομοθεσίας για τα θεμελιώδη δικαιώματα και τις ελευθερίες των πολιτών της ΕΕ, υπό το φως των νέων τεχνολογικών

---

[192] Ό.π.

[193] Ευρωπαϊκή Επιτροπή (2022) *Ο Βιομηχανικός Συνασπισμός Εικονικής και Επαυξημένης Πραγματικότητας.* Διαθέσιμο στο: https://digital-strategy.ec.europa.eu/el/policies/virtual-and-augmented-reality-coalition [Πρόσβαση 12 Μαΐου 2023].

εξελίξεων, ή θα παραστεί ανάγκη για αναθεώρησή της ή/και θέσπιση ειδικής νομοθεσίας για το Metaverse; Ποια τα προτεινόμενα μέτρα που ενδέχεται να μετριάσουν τις σαρωτικές επιπτώσεις της εμβύθισής μας σε έναν τρισδιάστατο εθιστικό κόσμο;

Η παρούσα διπλωματική εργασία θα επιχειρήσει να διερευνήσει τα εν λόγω ερωτήματα στο προσεχές κεφάλαιο, αναφορικά με τον τομέα των προσωπικών δεδομένων και ειδικότερα, τον Γενικό Κανονισμό για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα (ΕΕ) 2016/679.

Το νομοθετικό πλαίσιο της ΕΕ για την προστασία των προσωπικών δεδομένων είναι, ομολογουμένως, το πιο περιεκτικό και ισχυρό παγκοσμίως[194]. Την ίδια στιγμή, το πεδίο των προσωπικών δεδομένων είναι αυτό το οποίο θα υποστεί τις μεγαλύτερες προκλήσεις από την επικράτηση του Metaverse στην ενωσιακή αγορά. Οι λόγοι είναι κάτι παραπάνω από προβλέψιμοι.

Η είσοδος στο Metaverse θα συντελείται κατά βάση με τον ίδιο τρόπο που ένας χρήστης του Διαδικτύου συνδέεται σήμερα με τις ψηφιακές κοινότητες, απολαμβάνει ή παράγει ψηφιακό περιεχόμενο και χρησιμοποιεί ή προσφέρει ψηφιακές υπηρεσίες: μέσω των ψηφιακών πλατφορμών (digital platforms).

Οι ψηφιακές πλατφόρμες τροφοδοτούνται συνεχώς από δεδομένα, οργανώνονται και αυτοματοποιούνται μέσω διεπαφών λογισμικού και αλγορίθμων, διαμορφώνονται μέσω σχέσεων ιδιοκτησίας που υπαγορεύονται από επιχειρηματικά μοντέλα και διέπονται από νομικές συμφωνίες με τους χρήστες τους[195]. Αν και αρχικά δημιουργήθηκαν ως τεχνική λύση στα εγγενή προβλήματα της (ανάγκης) διαχείρισης δεδομένων[196], πολύ γρήγορα μεταμορφώθηκαν σε ιδιωτικά και ανταγωνιστικά εργοστάσια μαζικής εξαγωγής, συλλογής και επεξεργασίας δεδομένων των χρηστών τους. Τα δεδομένα αυτά χρησιμεύουν ως πρώτη ύλη για την παραγωγή και (χονδρική) πώληση του τελικού προϊόντος τους που δεν είναι άλλο από τα - εκτενή - προφίλ χρηστών. Η εξατομίκευση του προβαλλόμενου περιεχομένου που καθίσταται με αυτόν τον τρόπο δυνατή στις ψηφιακές πλατφόρμες, δεν αποτελεί τον αυτοσκοπό, αλλά το μέσο για τη μεγιστοποίηση των κερδών των οικείων παρόχων[197]. Ένα υποπροϊόν *("by-product")*[198] του ανταγωνισμού μεταξύ τους για την

[194] Kim, Y. (2022), σ. 228.

[195] Ό.π., Kalpokas, I. and Kalpokiene̋, J. (2023), σ. 6.

[196] Ό.π., σ. 19.

[197] Ό.π., σ. 22.

[198] Ό.π., σ. 25.

υπερσυγκέντρωση χρηστών και δεδομένων, η οποία καθορίζει την ποιότητα των παρεχόμενων υπηρεσιών τους, εμποδίζει την έξοδο των χρηστών από την πλατφόρμα τους και τελικά αποκλείει τους αντιπάλους από την είσοδο στη σχετική αγορά (network effects). Αδιαμφισβήτητα, η πλατφορμοποίηση *("platformisation")* του ψηφιακού περιβάλλοντος έχει συμβάλει ουσιωδώς στην αποδυνάμωση της ελεύθερης βούλησης και στην αντικειμενοποίηση των ανθρώπων[199]: τρίτοι γνωρίζουν τις προτιμήσεις μας, συν-διαμορφώνουν τις ανάγκες μας και πλουτίζουν εμπορευόμενοι τα δεδομένα μας.

Στο Metaverse, η εμβύθιση στις - εικονικές πλέον - πλατφόρμες θα οξύνει τα ήδη υπάρχοντα προβλήματα και θα εγείρει νέες, πρωτοφανείς προκλήσεις. Η ίδια η φύση του Metaverse ως ενός εμβυθιστικού 3D περιβάλλοντος μαρτυρά τη θέση των δεδομένων των χρηστών για τις οικείες πλατφόρμες ως εξ ορισμού αναγκαίων *("datafication by default")*[200]. Πολλώ δε μάλλον, η εμβύθιση θα διαμορφώσει τις συνθήκες για την ευρεία συλλογή και επεξεργασία δεδομένων που διαφορετικά θα ήταν αδύνατον να εξαχθούν[201]. Το Metaverse θα μοιάζει με το *Πανοπτικόν* του Jeremy Bentham, αλλά ενισχυμένο με το αναγκαίο κακό της τεχνολογικής προόδου· ενώ στο πρώτο ο κρατούμενος *ενδέχεται* να παρακολουθείται από *ένα* κεντρικό σημείο, στο Metaverse ο χρήστης *είναι δεδομένο* ότι θα παρακολουθείται *σε πραγματικό χρόνο* και από *πολλαπλά* σημεία *ταυτόχρονα*[202]. Όταν το Metaverse κατορθώσει να πετύχει το στόχο του, δηλαδή να εθίσει τους χρήστες και να τους προτρέψει να ζουν το μεγαλύτερο μέρος της ζωής τους εικονικά, τότε τα αποτελέσματα της υποβάθμισής τους από έμβια και έλλογα όντα σε άχαρα ψηφιδωτά δεδομένων θα είναι όχι μόνο εμφανή, αλλά και καταστροφικά. Μάλιστα, η αποσυναρμολόγηση αυτή του χρήστη σε bits δεδομένων θα γίνεται παρασκηνιακά και άρα εν αγνοία του, χάρη στην αυτοματοποίηση των εικονικών πλατφορμών μέσω των ενσωματωμένων σε αυτές αλγορίθμων Τεχνητής Νοημοσύνης. Στην εξίσωση πρέπει οπωσδήποτε να προσμετρηθεί το ότι οι πάροχοι που θα προσφέρουν την πρόσβαση στο Metaverse θα είναι κατ' εξοχήν ιδιωτικές εταιρείες με κίνητρο ίδια οικονομικά συμφέροντα. Σύμφωνα με τον Διευθύνοντα

[199] Ό.π., σ. 23.

[200] Ό.π., σ. 25.

[201] Ό.π., σ. 25.

[202] Ό.π., σ. 25.

Σύμβουλο της Epic Games, Tim Sweeny, *«αν μία κεντρική εταιρεία αποκτήσει τον έλεγχό του (Metaverse), θα γίνει πιο ισχυρή από οποιαδήποτε κυβέρνηση και θα είναι ο θεός στη Γη»*[203].

Η ανάγκη ρύθμισης του Metaverse για την προστασία των προσωπικών δεδομένων των χρηστών του είναι, συνεπώς, αδιαπραγμάτευτη. Μέλημα, λοιπόν, της ΕΕ είναι να απαντήσει στα καίρια ερωτήματα που διατυπώθηκαν νωρίτερα, με γνώμονα την εξισορρόπηση μεταξύ συγκρουόμενων - αν και όχι αλληλοαποκλειόμενων – δικαιωμάτων: αφενός μεν, της προστασίας των προσωπικών δεδομένων του ατόμου, αφετέρου δε, της ελεύθερης έκφρασης και ακώλυτης πρόσβασής του στην πληροφορία και της οικονομικής και κοινωνικής προόδου του συνόλου των πολιτών της, που η τεχνολογική ανάπτυξη και καινοτομία υπόσχεται ότι θα εξασφαλίσει. Ακολούθως, η παρούσα διπλωματική εργασία θα επιδιώξει να προσεγγίσει τα ανωτέρω ερωτήματα, σε σχέση με τις ιδιωτικής φύσεως πλατφόρμες Metaverse (private/hybrid).

[203] Marr, B. (2022) 'The 10 Best Metaverse Quotes Everyone Should Read', *Forbes*, 15 Αυγούστου. Διαθέσιμο στο: https://www.forbes.com/sites/bernardmarr/2022/08/15/the-10-best-metaverse-quotes-everyone-should-read/ [Πρόσβαση 12 Μαΐου 2023].

Β. ΣΚΙΑΓΡΑΦΩΝΤΑΣ ΤΙΣ ΝΟΜΙΚΕΣ ΠΡΟΚΛΗΣΕΙΣ ΤΟΥ METAVERSE ΥΠΟ ΤΟ ΦΩΣ ΤΟΥ ΓΚΠΔ

1. Η ΓΕΝΕΣΗ ΤΟΥ ΔΙΚΑΙΩΜΑΤΟΣ ΣΤΑ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ ΚΑΙ Η ΘΕΣΠΙΣΗ ΤΟΥ ΓΚΠΔ

Το δικαίωμα στην προστασία των προσωπικών δεδομένων[204] είχε διαπλαστεί στην Ευρώπη από τη νομολογία του Γερμανικού Ομοσπονδιακού Συνταγματικού Δικαστηρίου, ήδη από τα μέσα του 20ου αιώνα[205]. Μετέπειτα αναγνωρίστηκε αυτοτελώς, ως *μη απόλυτο* δικαίωμα, τόσο από εθνικές νομοθεσίες ευρωπαϊκών κρατών[206], όσο και από το Συμβούλιο της Ευρώπης[207] και την ΕΕ[208] [209]. Εντούτοις, η αλματώδης ανάπτυξη της τεχνολογίας και η εδραίωση των κοινωνικών δικτύων (social media) τη δεύτερη δεκαετία του 21ου αιώνα, επεσήμανε την αδήριτη ανάγκη περαιτέρω ρύθμισης, που υλοποιήθηκε τελικά το 2016, με την υιοθέτηση του Γενικού Κανονισμού για την Προστασία Δεδομένων Προσωπικού

---

[204] Συναντάται στη θεωρία και ως δικαίωμα πληροφοριακής ιδιωτικότητας, πληροφοριακής αυτοδιάθεσης ή πληροφοριακού αυτοκαθορισμού (βλ. Ακριβοπούλου, Χ. (2011) 'Το δικαίωμα στην προστασία των προσωπικών δεδομένων μέσα από το φακό του δικαιώματος στην ιδιωτική ζωή', *Θεωρία & Πράξη Διοικητικού Δικαίου*, 7/2011, σ. 683).

[205] 27 BVerfGE 1 (1969), 65 BVerfGE 1 (1984) (βλ. ό.π., σ. 682).

[206] Το πρώτο εθνικό νομοθέτημα για την προστασία των προσωπικών δεδομένων ήταν ο νόμος του γερμανικού κρατιδίου της Έσσης (1970). Ακολούθησε η θέσπιση συναφών νομοθεσιών σε Σουηδία (1973), Ομοσπονδιακή Δημοκρατία της Γερμανίας (1977) και Αυστρία, Γαλλία, Δανία, Νορβηγία (1978). Τα ως άνω νομοθετήματα χαρακτηρίζονται ως «πρώτης γενεάς» και τη δεκαετία του 1980, έδωσαν τη σκυτάλη σε «δεύτερης γενεάς» νομοθεσίες, στη Μ. Βρετανία, Ιρλανδία, Ολλανδία, Βέλγιο, Ισπανία και Πορτογαλία. Μετά την ψήφιση της Οδηγίας (ΕΚ) 95/46, εισήχθησαν πια νομοθετήματα «τρίτης γενεάς» στα ευρωπαϊκά κράτη (βλ. Ιγγλεζάκης, Ι. (2021) *Δίκαιο πληροφορικής*. Αθήνα-Θεσσαλονίκη: Εκδόσεις Σάκκουλα, Δ' έκδοση, σ. 325).

[207] Σύμβαση του Συμβουλίου της Ευρώπης 108, της 28ης Ιανουαρίου 1981, για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων.

[208] Βλ. άρθρο 8 του ΧΘΔΕΕ: «*1. Κάθε πρόσωπο έχει δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν. 2. Η επεξεργασία αυτών των δεδομένων πρέπει να γίνεται νομίμως, για καθορισμένους σκοπούς και με βάση τη συγκατάθεση του ενδιαφερομένου ή για άλλους θεμιτούς λόγους που προβλέπονται από το νόμο. Κάθε πρόσωπο δικαιούται να έχει πρόσβαση στα συλλεγέντα δεδομένα που το αφορούν και να επιτυγχάνει τη διόρθωσή τους. 3. Ο σεβασμός των κανόνων αυτών υπόκειται στον έλεγχο ανεξάρτητης αρχής*». Ομοίως, βλ. άρθρο 16 ΣΛΕΕ.

[209] Βλ. Οδηγία (ΕΚ) 95/46 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Οκτωβρίου 1995, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών.

Χαρακτήρα[210] (ΕΕ) 2016/679 (διεθνώς General Data Protection Regulation, εφεξής «ΓΚΠΔ»), ενός κειμένου με άμεση και καθολική εφαρμογή στα 28 τότε κράτη-μέλη της ΕΕ και ισχύ από τις 25 Μαΐου 2018[211] [212].

Το κείμενο του ΓΚΠΔ διαπνέεται από τεχνολογική ουδετερότητα, εφαρμόζεται, δηλαδή, ανεξάρτητα από το τεχνολογικό περιβάλλον και τις εκάστοτε χρησιμοποιούμενες τεχνικές επεξεργασίας των δεδομένων προσωπικού χαρακτήρα των υποκειμένων[213]. Συνεπώς, όπως έχει ήδη τονίσει και το Ευρωπαϊκό Κοινοβούλιο,[214] ο ΓΚΠΔ μπορεί κατ' αρχήν να ρυθμίσει την επεξεργασία των προσωπικών δεδομένων των χρηστών στο Metaverse, εντούτοις κρίνεται σκόπιμο να διερευνηθεί η προσφορότητά του να απαντήσει στις σχετικές νομικές προκλήσεις που αναμφίβολα θα εγείρει η επέκταση της ανθρώπινης δραστηριότητας σε ένα παράλληλο εικονικό σύμπαν.

2. Η ΕΦΑΡΜΟΓΗ ΤΟΥ ΓΚΠΔ ΣΤΟ METAVERSE

2.1 Ουσιαστικό πεδίο εφαρμογής

Το ερώτημα που διερευνάται σε αυτήν την ενότητα είναι αν (και γιατί) ο ΓΚΠΔ δύναται να εφαρμοστεί στο Metaverse. Μπορούν να θεωρηθούν ως «δεδομένα προσωπικού χαρακτήρα» κατά την έννοια των διατάξεων του ΓΚΠΔ, οι πληροφορίες που θα κοινοποιούν οι ίδιοι οι χρήστες (provided data), θα παρατηρούνται (observed data) ή θα συνάγονται (inferred data)[215] από τη συνολική δραστηριότητά τους κατά την εμβύθισή τους

---

[210] Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων).

[211] Ο ΓΚΠΔ ισχύει, επίσης, από τις 6 Ιουλίου 2018, σε Ισλανδία, Λιχτενστάιν και Νορβηγία (βλ. Κανέλλος, Λ. (2020) *THE GDPR HANDBOOK: για DPOs, Επιχειρήσεις & Οργανισμούς.* Αθήνα: Νομική Βιβλιοθήκη, σ. 1).

[212] Στην Ελλάδα, το δικαίωμα στην προστασία των προσωπικών δεδομένων ανυψώθηκε σε συνταγματικό δικαίωμα με την αναθεώρηση του Συντάγματος το 2001 και την προσθήκη του άρθρου 9[Α]. Σε εναρμόνιση με την κοινοτική Οδηγία (ΕΚ) 95/46, είχε ψηφισθεί, ήδη πριν τη συνταγματική αναθεώρηση, ο νόμος 2472/1997, ενώ σε εκτέλεση του ΓΚΠΔ υιοθετήθηκε στην ελληνική έννομη τάξη ο νόμος 4624/2019.

[213] Βλ. αιτιολογική σκέψη 15 ΓΚΠΔ.

[214] Ό.π., European Parliamentary Research Service (EPRS) (2022), σ. 6.

[215] Σύμφωνα με τη διάκριση που γίνεται επί τη βάσει της στόχευσης χρηστών κοινωνικών δικτύων, όπως επισημαίνεται από το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, Κατευθυντήριες

σε αυτό, ιδίως αν ληφθεί υπόψη η δυνατότητα αυτών να πλοηγούνται «ανώνυμα» στο εικονικό περιβάλλον; Με άλλα λόγια, μπορούν οι τελικοί χρήστες του να ταυτοποιηθούν - με τρόπο που να τους διαχωρίζει από τους υπόλοιπους - κατά την είσοδο και πλοήγησή τους στο Metaverse; Και αν ναι, και υπό ποιες άλλες προϋποθέσεις θα εφαρμόζεται ο ΓΚΠΔ;

Ο ΓΚΠΔ, κατά το άρθρο 2 παρ. 1 αυτού, εφαρμόζεται στην «*εν όλω ή εν μέρει, αυτοματοποιημένη επεξεργασία*[216] *δεδομένων προσωπικού χαρακτήρα*» φυσικών προσώπων, «*καθώς και στη μη αυτοματοποιημένη επεξεργασία τέτοιων δεδομένων τα οποία περιλαμβάνονται ή πρόκειται να περιληφθούν σε σύστημα αρχειοθέτησης*». Άρα, δεν προστατεύει δεδομένα νομικών προσώπων.

Το άρθρο 4 στοιχ. 1 ΓΚΠΔ ορίζει ως «δεδομένο προσωπικού χαρακτήρα» «*κάθε πληροφορία*[217] [218] *που αφορά*[219] *ταυτοποιημένο ή ταυτοποιήσιμο*[220] *φυσικό πρόσωπο*[221]

γραμμές 8/2020 σχετικά με τη στόχευση χρηστών μέσων κοινωνικής δικτύωσης, Έκδοση 2.0, της 13ης Απριλίου 2021. Διαθέσιμο στο: https://edpb.europa.eu/system/files/2021-11/edpb_guidelines_082020_on_the_targeting_of_social_media_users_el_0.pdf, σ. 16-17.

[216] Σύμφωνα με το άρθρο 4 στοιχ. 2 ΓΚΠΔ, ως «επεξεργασία» νοείται «*κάθε πράξη ή αλληλουχία πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή*».

[217] Δηλαδή, κάθε είδους δήλωση για ένα πρόσωπο. Ο όρος καλύπτει τόσο αντικειμενικές πληροφορίες, όπως το όνομα ή την παρουσία μιας συγκεκριμένης ουσίας στο αίμα του εν λόγω προσώπου, όσο και υποκειμενικές πληροφορίες, όπως γνώμες ή εκτιμήσεις (πχ. ο Α είναι αξιόπιστος δανειολήπτης). Είναι, επίσης, αδιάφορο αν οι πληροφορίες αυτές είναι αληθείς ή εσφαλμένες. (Βλ. Ομάδα προστασίας δεδομένων του άρθρου 29, Γνώμη 4/2007 σχετικά με την έννοια του όρου «δεδομένα προσωπικού χαρακτήρα», της 20ης Ιουνίου 2007. Διαθέσιμο στο https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_el.pdf, σ. 7).

[218] Οι πληροφορίες μπορούν να διατίθενται σε οποιαδήποτε μορφή (πχ. αλφαβητική, αριθμητική, γραφική, ακουστική, φωτογραφική κ.ά.) και σε οποιοδήποτε μέσο (πχ. χαρτί, μνήμη υπολογιστή κ.ά.) (βλ. ό.π., σ. 8).

[219] Με άλλα λόγια, κάθε πληροφορία που *σχετίζεται με* ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο. Τέτοιες είναι, φερ' ειπείν, οι πληροφορίες που περιλαμβάνονται στον ιατρικό φάκελο ορισμένου προσώπου, αλλά ενδέχεται να είναι και πληροφορίες που αφορούν σε αντικείμενα που ανήκουν, βρίσκονται πλησίον ή με οποιονδήποτε τρόπο επιδρούν σε ορισμένο πρόσωπο (βλ. ό.π., σ. 10).

[220] Ως ταυτοποιημένο ή ταυτοποιήσιμο χαρακτηρίζεται το φυσικό πρόσωπο που μπορεί να διακριθεί από τα υπόλοιπα, ώστε να μην προκαλείται σύγχυση ως προς την ταυτότητά του. Η διάκριση όμως αυτή δεν προϋποθέτει τη δυνατότητα ανεύρεσης του ονόματος του εν λόγω προσώπου (βλ. ό.π., σ.

(*«υποκείμενο των δεδομένων»*)», ενώ ως «ταυτοποιήσιμο φυσικό πρόσωπο» χαρακτηρίζεται «*εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό στοιχείο ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου*»[222]. Συνεπώς, όπως προβλέπεται και στην αιτιολογική σκέψη 26 ΓΚΠΔ, οι ανώνυμες πληροφορίες, μεταξύ των οποίων και τα ανωνυμοποιημένα δεδομένα φυσικών προσώπων, δεν συνιστούν δεδομένα προσωπικού χαρακτήρα κατά την έννοια του ΓΚΠΔ. Αντιθέτως, τα ψευδωνυμοποιημένα δεδομένα που μπορούν πράγματι να αποδοθούν σε συγκεκριμένο φυσικό πρόσωπο με τη χρήση πρόσθετων πληροφοριών προστατεύονται[223].

Περαιτέρω, σύμφωνα με το άρθρο 9 παρ. 1 ΓΚΠΔ, ειδική κατηγορία προσωπικών δεδομένων αποτελούν όσα «*αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, τα γενετικά δεδομένα, τα βιομετρικά δεδομένα και τα δεδομένα που αφορούν την υγεία, τη σεξουαλική ζωή ή τον γενετήσιο προσανατολισμό φυσικού προσώπου*».

Πάντως, ο ΓΚΠΔ *δεν* εφαρμόζεται στην επεξεργασία προσωπικών δεδομένων «*από φυσικό πρόσωπο στο πλαίσιο αποκλειστικά προσωπικής ή οικιακής δραστηριότητας*» (άρθρο

16-17 και Martin, B. (2022), σ. 259, *"the law covers even data that does not directly identify a named person if it could still help identify the "data subject.""*).

[221] Σύμφωνα με την αιτιολογική σκέψη 27 ΓΚΠΔ, δεν προστατεύει δεδομένα θανόντων. Ωστόσο, αν τα δεδομένα θανόντων αποκαλύπτουν προσωπικές πληροφορίες για ζώντα φυσικά πρόσωπα, τότε μόνον εμπίπτουν στο ουσιαστικό πεδίο εφαρμογής του ΓΚΠΔ.

[222] Άμεση είναι η ταυτοποίηση του φυσικού προσώπου που διενεργείται μέσω συγκεκριμένων προσωπικών δεδομένων, εφόσον ο εκάστοτε υπεύθυνος επεξεργασίας μπορεί να το ταυτοποιήσει επί τη βάσει μόνο αυτών των δεδομένων που διατηρεί για το υποκείμενο. Αντίθετα, έμμεση είναι η ταυτοποίηση όταν ο υπεύθυνος έχει τη δυνατότητα να το ταυτοποιήσει, μόνο κάνοντας χρήση συμπληρωματικών πληροφοριών που είτε διαθέτει ο ίδιος, είτε αναζητά από άλλη πηγή (βλ. ό.π., Kim, Y. (2022), σ. 242).

[223] Βλ. αιτιολογική σκέψη 26 ΓΚΠΔ, που αναφέρει ότι «*τα δεδομένα προσωπικού χαρακτήρα που έχουν υποστεί ψευδωνυμοποίηση, η οποία θα μπορούσε να αποδοθεί σε φυσικό πρόσωπο με τη χρήση συμπληρωματικών πληροφοριών, θα πρέπει να θεωρούνται πληροφορίες σχετικά με ταυτοποιήσιμο φυσικό πρόσωπο*» και άρα υπόκεινται στον ΓΚΠΔ. Μάλιστα, η εν λόγω αιτιολογική σκέψη ορίζει ότι για να διαπιστωθεί το κατά πόσο θα μπορούσαν πράγματι να χρησιμοποιηθούν (εφόσον υπάρχουν τα μέσα για τη συλλογή τους) συμπληρωματικές πληροφορίες για την ταυτοποίηση του φυσικού προσώπου, πρέπει να ληφθούν υπόψη αντικειμενικά κριτήρια, όπως ενδεικτικά, ο αναγκαίος χρόνος και τα έξοδα της διαδικασίας, σε συνάρτηση με τα τεχνολογικά μέσα της εποχής και τις τεχνολογικές εξελίξεις.

2 παρ. 2 στοιχ. γ')[224], παρόλα αυτά το ΔΕΕ έχει υπογραμμίσει ότι, όταν τα προσωπικά δεδομένα καθίστανται με αυτόν τον τρόπο προσβάσιμα σε απροσδιόριστο αριθμό προσώπων, ο κανόνας επανέρχεται και τα οικεία φυσικά πρόσωπα υπόκεινται στις διατάξεις του[225] [226].

Έτσι, λοιπόν, οι χρήστες του Metaverse, υπό τον όρο ότι είναι φυσικά πρόσωπα που δύναται να ταυτοποιηθούν με άμεσο ή έμμεσο τρόπο στον εικονικό κόσμο, θα αποτελούν «υποκείμενα» των δεδομένων κατά την έννοια του άρθρου 4 παρ. 1 ΓΚΠΔ, τα προσωπικά δεδομένα των οποίων θα χρήζουν προστασίας. Πρόσθετη προϋπόθεση για την εφαρμογή του ΓΚΠΔ είναι να συντελείται (η υπό τους όρους του άρθρου 2 παρ. 1 αυτού) επεξεργασία των προσωπικών δεδομένων τους από τρίτα μέρη, ακόμη και από φυσικά πρόσωπα, για σκοπούς που εκφεύγουν της αυστηρώς προσωπικής/οικιακής δραστηριότητας[227].

Για να εισέλθει στον εικονικό κόσμο, ο χρήστης θα πρέπει αρχικά να εγγραφεί σε μία οποιαδήποτε πλατφόρμα Metaverse, δηλαδή να ανοίξει έναν προσωπικό λογαριασμό και να κοινοποιήσει στον πάροχο αυτής διάφορες πληροφορίες που τον αφορούν και οι οποίες αποτελούν προσωπικά δεδομένα υπό το καθεστώς του ΓΚΠΔ, διότι μπορούν να οδηγήσουν σε κατ' αρχήν άμεση ταυτοποίησή του· ενδεικτικά, το ονοματεπώνυμό του (αναγνωριστικό στοιχείο ταυτότητας), την ημερομηνία γέννησής του, το φύλο του, τον

---

[224] Εντούτοις, ο ΓΚΠΔ εφαρμόζεται στους παρόχους της οικείας ψηφιακής υπηρεσίας (βλ. αιτιολογική σκέψη 18).

[225] Βλ. απόφαση ΔΕΕ C-101/01, Bodil Lindqvist, της 6ης Νοεμβρίου 2003. Διαθέσιμο στο: https://curia.europa.eu/juris/showPdf.jsf;jsessionid=CF52C9C21E43732093D105DEE15A44B1?text=&docid=48382&pageIndex=0&doclang=EL&mode=lst&dir=&occ=first&part=1&cid=14057586, αιτιολογική σκέψη 46.

[226] Όσον αφορά στα κοινωνικά δίκτυα, η Ομάδα προστασίας δεδομένων του άρθρου 29 είχε υποστηρίξει ότι η διατήρηση δημόσιου προφίλ από ένα φυσικό πρόσωπο καθιστά ανεφάρμοστη την εν λόγω διάταξη και το φυσικό πρόσωπο καταλαμβάνεται από τις διατάξεις της (τότε) Οδηγίας (ΕΚ) 95/46 (βλ. Ομάδα προστασίας δεδομένων του άρθρου 29, Γνώμη 5/2009 σχετικά με τις επιγραμμικές υπηρεσίες κοινωνικής δικτύωσης, της 12ης Ιουνίου 2009. Διαθέσιμο στο: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_el.pdf, σ. 7).

[227] Εκτός αν τα φυσικά αυτά πρόσωπα επεξεργάζονται προσωπικά δεδομένα τρίτων προσώπων στο Metaverse (πχ. ανεβάζουν φωτογραφίες τρίτων), ώστε αυτά να καθίστανται προσβάσιμα σε αόριστο αριθμό προσώπων (πχ. μέσω δημόσιων προφίλ). Απαιτείται περαιτέρω ρυθμιστική καθοδήγηση για το αν μπορεί να εφαρμοστεί η εξαίρεση στο περιβάλλον του Metaverse.

αριθμό κινητού τηλεφώνου του κ.ο.κ, αναλόγως των ρυθμίσεων της κάθε πλατφόρμας[228]. Οι πάροχοι, λοιπόν, των υπηρεσιών πλατφόρμας Metaverse θα είναι σε θέση να γνωρίζουν ακριβώς ποιος λογαριασμός και ποιος χρήστης δημιούργησε κάθε άβαταρ, επομένως οι χρήστες δεν θα μπορούν, εκ των πραγμάτων, να διατηρήσουν την ανωνυμία τους έναντι των παρόχων, παρά μόνο μια μορφή ψευδωνυμίας, αν το επιθυμούν[229]. Και σε αυτήν την περίπτωση, βέβαια, οι πάροχοι θα έχουν τα μέσα - και το κίνητρο - να εξακριβώσουν την πραγματική ταυτότητα των χρηστών[230].

Πέραν τούτων, οι πάροχοι θα είναι απαραίτητο να επεξεργάζονται και επιγραμμικά αναγνωριστικά στοιχεία ταυτότητας των χρηστών, όπως τη διεύθυνση του ηλεκτρονικού ταχυδρομείου τους (e-mail) ή τα αυτοεγκαθιστώμενα αρχεία cookies[231] [232]. Επίσης, θα είναι τεχνικά αναγκαίο ή σκόπιμο να επεξεργάζονται και μεταδεδομένα[233] που θα παράγονται κατά την πλοήγηση αυτών, ήτοι δεδομένα κίνησης, όπως είναι η διεύθυνση διαδικτυακού πρωτοκόλλου (IP address)[234], αλλά και δεδομένα θέσης[235], σε περίπτωση που ζητείται, για

---

[228] Καρδαμάκη, Α. (2022) 'Εικονικοί Κόσμοι, Metaverse και Προστασία Δεδομένων Προσωπικού Χαρακτήρα', *Επιθεώρηση Δικαίου Πληροφορικής*, 3(1). Διαθέσιμο στο: https://doi.org/10.26262/infolawj.v3i1.8907.

[229] Weingarden, G. and Artzt, M. (2022) 'Metaverse and privacy', *International Association of Privacy Professionals*, 23 Αυγούστου. Διαθέσιμο στο: https://iapp.org/news/a/metaverse-and-privacy-2/ [Πρόσβαση 23 Μαΐου 2023].

[230] Απαιτώντας, πχ., τη βιομετρική ταυτοποίησή τους (biometric authentication) πριν την είσοδό τους στην πλατφόρμα και όχι απλά την ταυτοποίηση αυτών με έναν κωδικό password ή PIN, ή συνδυάζοντας βιομετρικά δεδομένα από τις συσκευές XR, είτε τις παρέχουν οι ίδιοι ή τρίτοι.

[231] Ό.π., Καρδαμάκη, Α. (2022).

[232] Σύμφωνα με την αιτιολογική σκέψη 30 ΓΚΠΔ, τα αρχεία cookies μπορεί να αφήνουν διαδικτυακά ίχνη, τα οποία συνδυαστικά με μοναδικά αναγνωριστικά στοιχεία ταυτότητας και άλλες πληροφορίες που λαμβάνουν οι εξυπηρετητές, μπορούν να χρησιμοποιηθούν για να σκιαγραφηθεί το προφίλ των φυσικών προσώπων και να αναγνωριστεί η ταυτότητά τους.

[233] Βλ. άρθρο 4 παρ. 3 στοιχ. γ' της Πρότασης Κανονισμού (ΕΕ) του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 10ης Ιανουαρίου 2017, για τον σεβασμό της ιδιωτικής ζωής και την προστασία των δεδομένων προσωπικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες και την κατάργηση της οδηγίας 2002/58/ΕΚ (κανονισμός για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες) (διεθνώς ePrivacy Regulation, εφεξής «Πρόταση Κανονισμού ePrivacy»).

[234] Για το αν αποτελεί η διεύθυνση IP δεδομένο προσωπικού χαρακτήρα, βλ. απόφαση ΔΕΕ C-582/14, Patrick Breyer, της 19ης Οκτωβρίου 2016. Διαθέσιμο στο: https://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=el&mode=lst&dir=&occ=first&part=1&cid=946993, αιτιολογική σκέψη 49, η οποία έκρινε ότι η (δυναμική) διεύθυνση IP αποτελεί προσωπικό δεδομένο έναντι του παρόχου υπηρεσιών διαδικτύου, εφόσον αυτός έχει στη διάθεσή του νόμιμα μέσα για την εξακρίβωση της ταυτότητας του οικείου φυσικού προσώπου, χάρη στις πρόσθετες πληροφορίες που κατέχει για αυτό ο πάροχος υπηρεσιών πρόσβασης στο διαδίκτυο (Internet Service Provider/ISP).

παράδειγμα, η συναίνεση αυτών για τον γεωεντοπισμό τους, τη στιγμή δημιουργίας του λογαριασμού στην πλατφόρμα. Το ΔΕΕ έχει κρίνει με την Digital Rights Ireland[236] ότι τα μεταδεδομένα, ως προσωπικά δεδομένα τα οποία μόνο εμμέσως μπορούν να οδηγήσουν στην ταυτοποίηση του χρήστη, «*παρέχουν τη δυνατότητα συναγωγής ιδιαιτέρως ακριβών συμπερασμάτων σχετικά με τον ιδιωτική βίο των προσώπων των οποίων τα δεδομένα έχουν διατηρηθεί, όπως είναι οι καθημερινές συνήθειες, οι μόνιμοι ή οι προσωρινοί τόποι διαμονής, οι καθημερινές και άλλες μετακινήσεις, οι ασκούμενες δραστηριότητες, οι κοινωνικές σχέσεις των προσώπων αυτών και τα κοινωνικά περιβάλλοντα στα οποία τα πρόσωπα αυτά συχνάζουν*».

Από την άλλη, ο χρήστης θα χρησιμοποιεί αναγκαίως ειδικό εξοπλισμό, όπως VR headsets, smart glasses κλπ. (ή, στο πλέον δυστοπικό σενάριο, εμφυτεύσιμες διεπαφές εγκεφάλου - μηχανής), για να εμβυθιστεί στο εικονικό περιβάλλον. Ο σπουδαιότερος κίνδυνος που ελλοχεύει από τη χρήση τέτοιων εργαλείων εμβύθισης δεν είναι άλλος από τη συλλογή και επεξεργασία πληθώρας ευαίσθητων πληροφοριών[237], ιδίως βιομετρικών δεδομένων του τελικού χρήστη ή και τρίτων προσώπων - ικανών να ταυτοποιήσουν άμεσα ή έμμεσα τα οικεία φυσικά πρόσωπα -, που θα καταγράφονται και θα αποθηκεύονται από τις συσκευές αυτές μέσω ενσωματωμένου λογισμικού εγγραφής εικόνας, ήχου και άλλων αισθητήρων, κατά την πλοήγηση του χρήστη στο Metaverse. Σε επόμενη ενότητα (υπό 3.1.), το ζήτημα των προσωπικών δεδομένων που μπορούν να εξαχθούν χάρη στις συσκευές XR και τις παρεμφερείς τεχνολογίες θα αναλυθεί περαιτέρω.

Τέλος, ο χρήστης θα μπορεί να ταυτοποιηθεί, άμεσα ή έμμεσα, μέσω του άβαταρ που θα δημιουργήσει για να πλοηγείται στο τρισδιάστατο εμβυθιστικό σύμπαν. Τόσο τα χαρακτηριστικά και η εμφάνιση που θα προσδώσει στο άβατάρ του (πχ. όνομα χρήστη–

---

[235] Σύμφωνα με την Οδηγία (ΕΚ) 2002/58 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες) (διεθνώς ePrivacy Directive, εφεξής «Οδηγία ePrivacy»), ως «δεδομένα κίνησης» χαρακτηρίζονται «*τα δεδομένα που υποβάλλονται σε επεξεργασία για τους σκοπούς της διαβίβασης μιας επικοινωνίας σε δίκτυο ηλεκτρονικών επικοινωνιών ή της χρέωσής της*», ενώ ως «δεδομένα θέσης» χαρακτηρίζονται «*τα δεδομένα που υποβάλλονται σε επεξεργασία σε δίκτυο ηλεκτρονικών επικοινωνιών και που υποδεικνύουν τη γεωγραφική θέση του τερματικού εξοπλισμού του χρήστη μιας διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών*» (άρθρο 2 στοιχ. β' και γ' αντίστοιχα).

[236] Απόφαση ΔΕΕ C-293/12 και C-594/12, Digital Rights Ireland, της 8ης Απριλίου 2014. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/el/TXT/?uri=CELEX%3A62012CJ0293, αιτιολογική σκέψη 27.

[237] Ό.π., Κοντογεώργου, Π., Συρμακέζη, Ζ., Ζούλοβιτς, Μ. (2022), σ. 53.

username, φύλο, ηλικία, εθνικότητα, ντύσιμο, αξεσουάρ κ.ά.), όσο και η συμπεριφορά και η δραστηριότητα του άβαταρ εντός της πλατφόρμας (πχ. αντιδράσεις σε ερεθίσματα, διενέργεια οικονομικών συναλλαγών, κ.ά.), θα αποκαλύπτουν πληροφορίες ικανές να συνδέσουν την εικονική προσομοίωση με το φυσικό πρόσωπο πίσω από αυτή και άρα να ταυτοποιήσουν τον τελικό χρήστη κατά τρόπο που να τον διακρίνει από τους υπόλοιπους (θα αποτελούν δηλαδή - απλά[238] ή ευαίσθητα[239] - προσωπικά δεδομένα υπό το καθεστώς του ΓΚΠΔ), έστω κι αν κάποιες από τις πληροφορίες αυτές (πχ. username ή ηλικία) είναι επί τούτου ψευδωνυμοποιημένες[240] από τον πρώτο, με σκοπό να παραμείνει «ανώνυμος» στους υπόλοιπους χρήστες του δικτύου. Σε κάθε περίπτωση, και τα τρίτα αυτά μέρη θα έχουν τα μέσα[241], αλλά και το κίνητρο να εξακριβώσουν την ταυτότητα του χρήστη.

Όλα αυτά τα δεδομένα (και ομοίως, πολλά άλλα), ως πληροφορίες που αφορούν σε ταυτοποιήσιμα φυσικά πρόσωπα τα οποία πρόκειται να συμμετέχουν στην εμβυθιστική εμπειρία του Metaverse, χαρακτηρίζονται ως «δεδομένα προσωπικού χαρακτήρα» κατά την έννοια του ΓΚΠΔ. Επιπλέον, θα υπόκεινται συνεχώς σε αυτοματοποιημένη επεξεργασία, κυρίως από τους αλγορίθμους Τεχνητής Νοημοσύνης των διαφόρων εμπλεκόμενων μερών, προς εξυπηρέτηση επαγγελματικών, εμπορικών και επιχειρηματικών, πολιτικών ή άλλων παρεμφερών συμφερόντων τους, επισύροντας την άμεση εφαρμογή του ΓΚΠΔ για τις οντότητες εκείνες οι δραστηριότητες επεξεργασίας των οποίων υπόκεινται συνάμα στο εδαφικό πεδίο εφαρμογής του.

2.2. Εδαφικό πεδίο εφαρμογής

Πριν την υλοποίηση του Metaverse, είναι σημαντικό να αποσαφηνιστεί ποια ή ποιες νομοθεσίες περί ιδιωτικότητας πρόκειται να ρυθμίσουν την επεξεργασία των προσωπικών δεδομένων των χρηστών που θα συντελείται σε αυτό.

---

[238] Για παράδειγμα, οι οικονομικές συναλλαγές του χρήστη θα μπορούν να φανερώσουν τον αριθμό του τραπεζικού λογαριασμού ή της χρεωστικής κάρτας του, ενώ οι κοινωνικές επαφές του τον στενό ή ευρύτερο κοινωνικό του περίγυρο.

[239] Για παράδειγμα, το ντύσιμο και τα αξεσουάρ του άβαταρ θα μπορούν να αποκαλύπτουν πληροφορίες για τη σεξουαλική ζωή ή το γενετήσιο προσανατολισμό του χρήστη.

[240] Ό.π., Weingarden, G. and Artzt, M. (2022).

[241] Συνδυάζοντας την πληθώρα δεδομένων που θα αποκτούν για τους χρήστες, μεταξύ άλλων, μέσω του άβατάρ τους.

Το σίγουρο είναι ότι κάθε υπόχρεος φορέας θα υπόκειται σε πλήθος διαφορετικών νομικών κανόνων περί ιδιωτικότητας[242], ανάλογα με την εκάστοτε πραγματοποιούμενη επεξεργασία, αφού οι σχετικές παρεχόμενες υπηρεσίες δεν θα περιορίζονται σε μία μόνο δικαιοδοσία, αλλά ενδέχεται να διαχέονται ταυτόχρονα σε ολόκληρο τον πλανήτη[243]. Ακόμη και τα ίδια υποκείμενα ή τα ίδια δεδομένα είναι δυνατόν να υπόκεινται σε διαφορετικά ρυθμιστικά πλαίσια περί ιδιωτικότητας, καθιστώντας προβληματική την ορθή εφαρμογή των οικείων κανόνων[244].

Εξαιτίας των ως άνω, είναι πολύ πιθανό ορισμένες πλατφόρμες να συμπεριλάβουν στους Όρους Παροχής Υπηρεσιών τους ρήτρες εφαρμοστέου δικαίου, οι οποίες όμως, σε περίπτωση που αντιβαίνουν σε αναγκαστικού δικαίου διατάξεις νόμων, θα κρίνονται τελικά ως άκυρες και ανεφάρμοστες[245].

Στο πλαίσιο αυτό, κρίσιμο είναι να εξεταστεί το εδαφικό πεδίο εφαρμογής του ΓΚΠΔ. Δυνάμει του άρθρου 3 ΓΚΠΔ, δύο είναι τα κριτήρια εκείνα που καθορίζουν αν μία συγκεκριμένη επεξεργασία υπόκεινται στο ρυθμιστικό πλαίσιό του: (α) το κριτήριο της εγκατάστασης, της παρ. 1 του άρθρου 3 και (β) το κριτήριο της στόχευσης, της παρ. 2 του άρθρου 3.

Σύμφωνα με το κριτήριο της εγκατάστασης, ο ΓΚΠΔ εφαρμόζεται κατ' αρχήν σε κάθε «*επεξεργασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο των δραστηριοτήτων μιας εγκατάστασης ενός υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία στην Ένωση, ανεξάρτητα από το κατά πόσο η επεξεργασία πραγματοποιείται εντός της Ένωσης*».

Ο όρος «εγκατάσταση» έχει εδώ την έννοια της «*ουσιαστικής και πραγματικής άσκησης δραστηριότητας μέσω σταθερών ρυθμίσεων, ο νομικός τύπος των οποίων, είτε πρόκειται για παράρτημα είτε για θυγατρική με νομική προσωπικότητα, δεν είναι*

---

[242] Δεν υπάρχει ομοιόμορφο νομοθετικό καθεστώς για την προστασία των προσωπικών δεδομένων σε παγκόσμιο επίπεδο. Στις ΗΠΑ, για παράδειγμα, το βασικό νομοθέτημα σε ομοσπονδιακό επίπεδο είναι η Privacy Act του 1974, αλλά υπάρχει και ειδική τομεακή νομοθεσία, όπως η Health Insurance Portability and Accountability Act (HIPAA), σχετικά με τα προσωπικά δεδομένα υγείας. Επιπλέον, ορισμένες Πολιτείες έχουν θεσπίσει τους δικούς τους νόμους περί προστασίας προσωπικών δεδομένων, όπως είναι η California Consumer Privacy Act (CCPA) και η Virginia Consumer Data Protection Act (CDPA).

[243] Έτσι, για παράδειγμα, χρήστες από οποιαδήποτε γωνιά της Γης θα μπορούν να συγκεντρώνονται ταυτόχρονα σε ένα εικονικό νυχτερινό κέντρο διασκέδασης, καθένας εκ των οποίων θα υπόκειται σε διαφορετικό καθεστώς ιδιωτικότητας (βλ. ό.π., Weingarden, G. and Artzt, M. (2022)).

[244] Ό.π., Κουσουνή-Πανταζοπούλου (2023), σ. 381.

[245] Ό.π., Weingarden, G. and Artzt, M. (2022).

καθοριστικής σημασίας»[246]. Καίριος είναι ο βαθμός μονιμότητας της εγκατάστασης[247], καθώς επίσης ο ουσιαστικός χαρακτήρας της άσκησης δραστηριοτήτων εντός κράτους-μέλους της ΕΕ[248] [249].

Η επεξεργασία, τώρα, των προσωπικών δεδομένων πρέπει να λαμβάνει χώρα είτε από την ίδια την εγκατάσταση εντός ΕΕ, είτε από άλλη εγκατάσταση του υπευθύνου ή εκτελούντος εκτός ΕΕ «*στο πλαίσιο των δραστηριοτήτων της εγκατάστασης* εντός ΕΕ»[250] [251], γεγονός που επιβεβαιώνει τον ισχυρισμό ότι είναι νομικά αδιάφορος ο τόπος της πραγματοποιηθείσας επεξεργασίας. Αδιάφορη είναι, επίσης, νομικά και η ιθαγένεια ή ο τόπος διαμονής των υποκειμένων τα δεδομένα των οποίων υφίστανται επεξεργασία, σύμφωνα και με την αιτιολογική σκέψη 14 ΓΚΠΔ[252].

Εκ των ανωτέρω, προκύπτει με σαφήνεια ότι μελλοντικά, οποιαδήποτε οντότητα δραστηριοποιείται στο Metaverse, εφόσον διαθέτει εγκατάσταση στην Ένωση - τηρούμενων των ως άνω προϋποθέσεων - και επεξεργάζεται προσωπικά δεδομένα χρηστών υπό την ιδιότητά της ως υπεύθυνου ή εκτελούντος την επεξεργασία, είτε μέσω της εγκατάστασης αυτής ή, τουλάχιστον, στο πλαίσιο των δραστηριοτήτων της εν λόγω εγκατάστασης, θα υπόκειται άνευ άλλου τινός στις διατάξεις του ΓΚΠΔ αναφορικά με τη συγκεκριμένη επεξεργασία.

Περαιτέρω, σύμφωνα με το κριτήριο της στόχευσης, ο ΓΚΠΔ εφαρμόζεται για κάθε «*επεξεργασία δεδομένων προσωπικού χαρακτήρα υποκειμένων των δεδομένων που βρίσκονται στην Ένωση από υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία μη*

---

[246] Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, Κατευθυντήριες γραμμές 3/2018 σχετικά με το εδαφικό πεδίο εφαρμογής του ΓΚΠΔ (άρθρο 3), Έκδοση 2.1, της 12ης Νοεμβρίου 2019. Διαθέσιμο στο: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_consultation_el.pdf, σ. 6-7.

[247] Έχει κριθεί ότι ακόμη κι η παρουσία ενός μόνο υπαλλήλου ή αντιπροσώπου του φορέα με εγκατάσταση εκτός ΕΕ στην Ένωση, ενδέχεται υπό όρους να πληροί τις προϋποθέσεις της μόνιμης εγκατάστασης (βλ. ό.π., σ. 7).

[248] Ό.π.

[249] Έχει κριθεί ότι απλώς και μόνο η ύπαρξη ιστοτόπου προσβάσιμου από το οικείο κράτος-μέλος δεν συνιστά άνευ άλλου τινός εγκατάσταση εντός ΕΕ (βλ. ό.π., σ. 7-8).

[250] Ό.π., σ. 8.

[251] Για τα ειδικότερα κριτήρια βάσει των οποίων μια εγκατάσταση εκτός ΕΕ θεωρείται ότι επεξεργάζεται δεδομένα προσωπικού χαρακτήρα φυσικών προσώπων, στο πλαίσιο της τοπικής εγκατάστασης εντός ΕΕ, βλ. ό.π., σ. 9-10.

[252] *«Η προστασία που παρέχει ο παρών κανονισμός θα πρέπει να ισχύει για τα φυσικά πρόσωπα, ανεξαρτήτως ιθαγένειας ή τόπου διαμονής, σε σχέση με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα τους».*

εγκατεστημένο στην Ένωση, εάν οι δραστηριότητες επεξεργασίας σχετίζονται με: α) την προσφορά αγαθών ή υπηρεσιών[253] *στα εν λόγω υποκείμενα των δεδομένων στην Ένωση, ανεξαρτήτως εάν απαιτείται πληρωμή από τα υποκείμενα των δεδομένων, ή β) την παρακολούθηση της συμπεριφοράς τους, στον βαθμό που η συμπεριφορά αυτή λαμβάνει χώρα εντός της Ένωσης».*

Με λίγα λόγια, δηλαδή, η οικεία επεξεργασία καταλαμβάνεται από τις διατάξεις του ΓΚΠΔ, ακόμη κι όταν οι υπόχρεοι δεν είναι εγκατεστημένοι στην Ένωση, αλλά τα υποκείμενα των δεδομένων που υπόκεινται στην εν λόγω επεξεργασία βρίσκονται στην Ένωση και οι υπόχρεοι στοχεύουν τα εν λόγω υποκείμενα, παρέχοντάς τους προϊόντα ή υπηρεσίες ή παρακολουθώντας τη συμπεριφορά τους.

Σημασία έχει, κατά συνέπεια, η γεωγραφική θέση των υποκειμένων τη χρονική στιγμή της προσφοράς των αγαθών ή υπηρεσιών ή της διενέργειας της παρακολούθησης και όχι η ιθαγένεια, ο τόπος διαμονής ή άλλο νομικό καθεστώς που τα αφορά[254], ενώ η στόχευση των υποκειμένων που βρίσκονται στην Ένωση πρέπει να υλοποιείται εκ προθέσεως (στην περίπτωση της παρακολούθησης, η πρόθεση στόχευσης τεκμαίρεται) και όχι ακούσια ή συμπτωματικά[255], όπως συμβαίνει, φερ' ειπείν, όταν ένας φορέας στοχεύει υποκείμενα εκτός ΕΕ, αλλά η παρεχόμενη από αυτόν υπηρεσία δεν ανακαλείται όταν τα υποκείμενα εισέρχονται εντός ΕΕ[256].

Όσον αφορά στην έννοια της παρακολούθησης, η αιτιολογική σκέψη 24 του ΓΚΠΔ θεσπίζει ότι θα πρέπει να ερευνάται αν τα υποκείμενα των δεδομένων παρακολουθούνται

---

[253] Στις εν λόγω υπηρεσίες συγκαταλέγονται και οι υπηρεσίες της Κοινωνίας της Πληροφορίας, που ορίζονται ως «*οποιαδήποτε υπηρεσία της κοινωνίας των πληροφοριών, ήτοι κάθε υπηρεσία που συνήθως παρέχεται έναντι αμοιβής, με ηλεκτρονικά μέσα εξ αποστάσεως και κατόπιν συγκεκριμένης παραγγελίας ενός αποδέκτη υπηρεσιών*» στο άρθρο 1 παρ. 1 στοιχ. β' της Οδηγίας (ΕΕ) 2015/1535 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 9ης Σεπτεμβρίου 2015, για την καθιέρωση μιας διαδικασίας πληροφόρησης στον τομέα των τεχνικών προδιαγραφών και των κανόνων σχετικά με τις υπηρεσίες της κοινωνίας των πληροφοριών.

[254] Ό.π., Κατευθυντήριες γραμμές 3/2018, σ. 18.

[255] Για τις προϋποθέσεις υπό τις οποίες δύναται να συναχθεί η βούληση του φορέα να κατευθύνει την προσφορά αγαθών ή υπηρεσιών σε υποκείμενα εντός της ΕΕ, βλ. ό.π., σ. 21-24. Ενδεικτικά, η συναφής βούληση πιθανολογείται σε περιπτώσεις, όπως η χρήση γλώσσας και νομίσματος κράτους-μέλους από ιστότοπο παρόχου, συνδυαστικά με τη δυνατότητα παραγγελίας σε αυτή τη γλώσσα, η δυνατότητα παράδοσης αγαθών σε κράτος –μέλος, η χρήση διαφορετικού (πχ. ".de", ".gr" κλπ.) ή ουδέτερου (πχ. ".eu" κλπ.) domain-name από εκείνο της τρίτης χώρας, η πληρωμή φορέα εκμετάλλευσης μηχανής αναζήτησης για την παροχή υπηρεσιών ευρετηρίασης, προκειμένου να διευκολύνεται η παροχή της πρόσβασης στον οικείο ιστότοπο σε χρήστες στην ΕΕ κ.ο.κ.

[256] Ό.π., σ. 18.

μέσω Διαδικτύου[257], συμπεριλαμβανομένης της μετέπειτα *δυνητικής* χρήσης τεχνικών κατάρτισης προφίλ, ιδίως για τη λήψη αποφάσεων που τα αφορούν, την ανάλυση ή την πρόβλεψη των προσωπικών προτιμήσεων, των συμπεριφορών και των νοοτροπιών τους (πχ. συμπεριφορική διαφήμιση, γεωεντοπισμός με στόχο το marketing κ.ο.κ). Άρα, η πλήρωση του κριτηρίου της παρακολούθησης των υποκειμένων στο Metaverse τεκμαίρεται.

Ως εκ των ανωτέρω, καθίσταται σαφές ότι οι πάροχοι υπηρεσιών σχετικών με το Metaverse, έστω κι αν δεν είναι εγκατεστημένοι εντός ΕΕ, θα καταλαμβάνονται ως προς ορισμένες δραστηριότητες επεξεργασίας προσωπικών δεδομένων από τις εξωεδαφικές διατάξεις του ΓΚΠΔ, εφόσον πληρούν το κριτήριο της στόχευσης υποκειμένων που βρίσκονται στην Ένωση, είτε παρέχοντάς τους εκ προθέσεως προϊόντα ή υπηρεσίες είτε, σε κάθε περίπτωση, παρακολουθώντας τη συμπεριφορά τους, εφόσον το αντίστοιχο προϊόν ή η υπηρεσία εξακολουθεί να λειτουργεί εντός της ενωσιακής αγοράς.

Πάντως, θα είναι χρήσιμο, αν όχι αναγκαίο, οι σχετικές Κατευθυντήριες Γραμμές για το εδαφικό πεδίο εφαρμογής του ΓΚΠΔ να αναθεωρηθούν και εξειδικευθούν, ώστε να αποσαφηνίσουν τον τρόπο εφαρμογής των συναφών κριτηρίων της εγκατάστασης και της στόχευσης στο εικονικό περιβάλλον.

3. ΕΙΔΙΚΑ ΖΗΤΗΜΑΤΑ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΟ METAVERSE

3.1. Επεξεργασία προσωπικών δεδομένων εξαγόμενων από συσκευές XR και παρεμφερείς τεχνολογίες

Τα προσωπικά δεδομένα των χρηστών του Metaverse δεν θα συνιστούν απλώς καύσιμη ύλη, αλλά νευραλγικό δομικό στοιχείο του εικονικού κόσμου[258].

Τα ευρήματα του Business Insider του 2022 για τη Meta Platforms επιβεβαιώνουν την κομβική σημασία των προσωπικών δεδομένων για τις εταιρείες που θα δραστηριοποιηθούν στο χώρο: εξετάζοντας εκατοντάδες σχετικές αιτήσεις που υποβλήθηκαν από την εταιρεία προς έγκριση στο Γραφείο Διπλωμάτων Ευρεσιτεχνίας και Εμπορικών Σημάτων των ΗΠΑ

[257] Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων έχει υποστηρίξει ότι η αναφορά στο Διαδίκτυο ως τεχνολογίας που επιτρέπει την παρακολούθηση είναι ενδεικτική και έτσι, π.χ., φορέσιμες (wearables) και εν γένει έξυπνες συσκευές (smart devices) εμπίπτουν ομοίως στην έννοια της παρακολούθησης, σύμφωνα με το πνεύμα του ΓΚΠΔ (βλ. ό.π., σ. 24).

[258] Ό.π., Anidjar, L.Y., Packin, N.G. and Panezi, A. (2023), σ. 18.

(US Patent and Trademark Office/USPTO), αποκάλυψε ότι στόχος της είναι να δημιουργήσει υπερ-ρεαλιστικά άβαταρ, προσομοιώνοντας κάθε πόρο δέρματος, κάθε στέλεχος τρίχας και κάθε ανεπαίσθητη κίνηση των χρηστών[259].

Ο ειδικός εξοπλισμός εμβύθισης που θα χρησιμοποιείται από τους τελευταίους για να εισέλθουν στον εικονικό κόσμο (πχ. VR headsets, smart glasses, haptic gloves, haptic bodysuits, BCI κλπ.), θα έχει πράγματι την ικανότητα να καταγράφει και να αποθηκεύει έναν πλούτο προσωπικών δεδομένων, κυρίως ευαίσθητων, μέσω ενσωματωμένων έξυπνων καμερών, ηχείων ή/και λοιπών αισθητήρων[260]. Τα δεδομένα αυτά διακρίνονται ως εξής:

1. Δεδομένα θέσης (location data): Οι συσκευές XR θα χρειάζεται να εντοπίζουν την ακριβή θέση του χρήστη στο χώρο, οι VR για να διασφαλίζουν την ασφάλειά του, ότι δηλαδή δεν θα συγκρουστεί με περιφερειακά αντικείμενα ή επιφάνειες, οι AR για να αναπαράγουν το σχετικό ψηφιακό υπόστρωμα[261]. Για το λόγο αυτό, θα είναι αναγκαίο να επεξεργάζονται σχετικές πληροφορίες, όπως είναι όσες προκύπτουν από το Παγκόσμιο Σύστημα Στιγματοθέτησης (Global Positioning System/GPS), την Αδρανειακή Μονάδα Μέτρησης (Inertial Measurement Unit/IMU) και γενικότερα διάφορους αισθητήρες κίνησης[262] (πχ. γυροσκόπιο-gyroscope, επιταχυνσιόμετρο-accelerometer, μαγνητόμετρο-magnetometer κ.ο.κ.), οι οποίες ανήκουν στα απλά προσωπικά δεδομένα υπό το καθεστώς του ΓΚΠΔ. Από αυτά, οι οικείοι πάροχοι θα μπορούν να συνάγουν και άλλα προσωπικά δεδομένα για το χρήστη, όπως είναι ο τόπος κατοικίας ή διαμονής, το ταξικό υπόβαθρό του κ.ά.

2. Χωρικά δεδομένα (spatial data): Ταυτόχρονα, προς τους ανωτέρω σκοπούς, τα ειδικά εργαλεία εμβύθισης θα συλλέγουν δεδομένα για τον περιβάλλοντα χώρο του χρήστη[263] (πχ. μέσω ενσωματωμένων καμερών με κατεύθυνση προς τα έξω στη διάταξη οπτικής προβολής HMD[264]) και άρα, για τα αντικείμενα ή τα πρόσωπα που τυχαίνει να

---

[259] Ό.π., Martin, B. (2022), σ. 247.

[260] Ό.π., Nextrope (2022), σ. 20.

[261] Ό.π., Dick, E. (2021), σ. 7.

[262] Ό.π.

[263] Fernandez, C. B. and Hui, P. (2022) 'Life, the Metaverse and Everything: An Overview of Privacy, Ethics, and Governance in Metaverse', *2022 IEEE 42nd International Conference on Distributed Computing Systems Workshops (ICDCSW)*, Μπολόνια, Ιταλία, 10 Ιουλίου. IEEE, σ. 272-277. Διαθέσιμο στο: https://doi.org/10.1109/icdcsw56584.2022.00058, σ. 273 και ό.π., Dick, E. (2021), σ. 7.

[264] Ό.π., Dick, E. (2021).

βρίσκονται εντός του, αλλά και για τις ιδιωτικές συνομιλίες αυτού και των γύρω του[265]. Ως αποτέλεσμα, οι πάροχοι θα έχουν πρόσβαση σε προσωπικά δεδομένα του παρατηρούμενα/συναγόμενα[266] από την οπτική ή ηχητική καταγραφή του ιδιωτικού του χώρου (πχ. οικογενειακή και οικονομική κατάσταση κλπ.), ορισμένα εκ των οποίων ενδεχομένως να εμπίπτουν στην έννοια των ευαίσθητων (πχ. σεξουαλική ζωή, πολιτικές και θρησκευτικές πεποιθήσεις[267] κλπ.), σε προσωπικά δεδομένα, ακόμη και ευαίσθητα (πχ. βιομετρικά δεδομένα και δεδομένα υγείας[268] κλπ.), τρίτων προσώπων (non-users) που ούτε γνωρίζουν ούτε συναινούν[269], βεβαίως, σε μια τέτοια επεξεργασία[270], και τέλος, σε περιεχόμενο και μεταδεδομένα επικοινωνίας, που προστατεύονται από το απόλυτο δικαίωμα στο απόρρητο των επικοινωνιών κατά τις διατάξεις της Οδηγίας και της Πρότασης Κανονισμού ePrivacy και που μπορούν, επίσης, να αποκαλύψουν πλήθος προσωπικών δεδομένων για τους χρήστες και τους οικείους τους κατά την έννοια του ΓΚΠΔ. Αναντίρρητα, η πρόσβαση σε όλα αυτά τα δεδομένα θα μπορεί να οδηγήσει σε μια άνευ προηγουμένου διείσδυση στην ιδιωτική σφαίρα του ατόμου.

3. Βιομετρικά δεδομένα εν ευρεία εννοία:

(α) Βιομετρικά δεδομένα εν στενή εννοία (biometric data): Στο Metaverse, οι συσκευές XR και οι παρεμφερείς τεχνολογίες θα επιτρέπουν την άμεση ταυτοποίηση του χρήστη, μέσω ειδικής τεχνικής επεξεργασίας μοναδικών για κάθε άνθρωπο χαρακτηριστικών[271], όπως της ίριδας του ματιού, του αμφιβληστροειδούς χιτώνα, της ανατομίας του προσώπου, του ηχοχρώματος της φωνής, του μοτίβου βάδισης, του

---

[265] Lumley, C. (2022) 'Data protection in the metaverse', *Lexology*. 27 Οκτωβρίου. Διαθέσιμο στο: https://www.lexology.com/library/detail.aspx?g=335a2e93-8ba3-46e5-9988-4c0c04b54d89 [Πρόσβαση 23 Μαΐου 2023].

[266] Σύμφωνα με τη Γνώμη 4/2007 της Ομάδας προστασίας δεδομένων του άρθρου 29 για την προηγούμενη Οδηγία (ΕΚ) 95/46, ως προσωπικά δεδομένα μπορούν να θεωρηθούν και τα ίδια τα αντικείμενα που ανήκουν στον περιβάλλοντα χώρο του χρήστη, καθώς μέσω αυτών ενδέχεται να αξιολογηθεί, να αντιμετωπιστεί με έναν ορισμένο τρόπο ή να επηρεασθεί η κατάσταση ή η συμπεριφορά του (βλ. ό.π., Καρδαμάκη, Α. (2022)).

[267] Πχ. όταν στο χώρο καταγράφονται θρησκευτικές εικόνες κ.ο.κ.

[268] Πχ. όταν στο χώρο καταγράφεται ο συγκάτοικος του χρήστη, ο οποίος βρίσκεται σε αναπηρικό αμαξίδιο.

[269] Ό.π., Lumley, C. (2022).

[270] European Data Protection Supervisor (2019) *Technology Report No 1: Smart glasses and data protection.* Βρυξέλλες: European Data Protection Supervisor. Διαθέσιμο στο: https://edps.europa.eu/sites/edp/files/publication/19-01-18_edps-tech-report-1-smart_glasses_en.pdf, σ. 6.

[271] Βλ. ό.π., Mangada Real de Asúa, E. et al. (2022), σ. 15.

δακτυλικού αποτυπώματος ή/και της φλεβικής διάταξής του κ.ο.κ. (πχ. βιομετρική ταυτοποίηση για σκοπούς ασφαλείας ή για την επιβεβαίωση της ηλικίας του χρήστη, με τη χρήση τεχνολογιών αναγνώρισης προσώπου-face recognition, σάρωσης της ίριδας ή του δακτυλικού αποτυπώματος-iris/fingerprint scanning κ.ά.). Ο ΓΚΠΔ ορίζει ως βιομετρικά δεδομένα υπό την έννοια του άρθρου 9 παρ. 1 για τα ευαίσθητα «*όσα προκύπτουν από ειδική τεχνική επεξεργασία συνδεόμενη με φυσικά, βιολογικά ή συμπεριφορικά χαρακτηριστικά φυσικού προσώπου και τα οποία επιτρέπουν ή επιβεβαιώνουν την αδιαμφισβήτητη ταυτοποίηση του εν λόγω φυσικού προσώπου, όπως εικόνες προσώπου ή δακτυλοσκοπικά δεδομένα*» (άρθρο 4 παρ. 14). Τα κριτήρια, λοιπόν, για τον χαρακτηρισμό των δεδομένων ως βιομετρικών είναι (α) η φύση των δεδομένων (να σχετίζονται με φυσικά, βιολογικά ή συμπεριφορικά χαρακτηριστικά φυσικού προσώπου), (β) τα μέσα και ο τρόπος της επεξεργασίας (να προκύπτουν από ειδική τεχνική επεξεργασία) και (γ) ο σκοπός της επεξεργασίας (να χρησιμοποιούνται με σκοπό την *αδιαμφισβήτητη* ταυτοποίηση φυσικού προσώπου), τα οποία πρέπει να συντρέχουν σωρευτικά[272]. Έτσι, όλα τα ανωτέρω δεδομένα αδιαμφισβήτητα θα εμπίπτουν στην έννοια των ευαίσθητων βιομετρικών δεδομένων των άρθρων 9 παρ. 1 και 4 παρ. 14 ΓΚΠΔ και θα χαίρουν αυξημένης προστασίας υπό το ισχύον νομοθετικό καθεστώς.

Παράλληλα, το υλισμικό εμβύθισης θα επιτρέπει την επεξεργασία και βιομετρικών δεδομένων τα οποία μόνο εμμέσως θα μπορούν να ταυτοποιήσουν το χρήστη, όπως είναι πχ. οι μεμονωμένες κινήσεις του κεφαλιού, του σώματος και των χεριών του (μέσω τεχνολογιών εντοπισμού της κίνησης αυτών-head/body/hand tracking), με σκοπό την αναπαραγωγή των κινήσεών του στο εικονικό περιβάλλον. Οι εξελιγμένες διατάξεις κεφαλής VR ήδη ενσωματώνουν εργαλεία που εντοπίζουν και αναπαράγουν τις κινήσεις των χρηστών με 6 βαθμούς ελευθερίας (six degrees of freedom/6DoF), έτσι ώστε ο χρήστης να μπορεί να κουνήσει το κεφάλι του πάνω-κάτω, δεξιά-αριστερά και από πλευρά σε πλευρά, αλλά και να σηκωθεί όρθιος-να καθίσει κάτω, να στρίψει το σώμα του δεξιά-αριστερά και να προχωρήσει μπρος-πίσω[273]. Πράγματι, ενώ η κίνηση μίας μεμονωμένης άρθρωσης δεν οδηγεί σε άμεση ταυτοποίησή του, μία αλληλουχία κινήσεων του σώματος που υποδεικνύει το «*πώς κάποιος κινείται, συντονίζει και χρησιμοποιεί τα μέρη του σώματός*

[272] Βλ. Κατευθυντήριες γραμμές 3/2019 σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα μέσω βιντεοσυσκευών, Έκδοση 2.0, της 29 Ιανουαρίου 2020, σ. 21.

[273] Ό.π., Dick, E. (2021), σ. 7.

του μεταξύ τους», μπορεί κάλλιστα να τον ταυτοποιήσει, μέσω ειδικών τεχνικών ανάλυσης και με ποσοστό επιτυχίας περίπου 60%[274]. Σύμφωνα με άλλη έρευνα, η παρακολούθηση των υποκειμένων μέσω τεχνολογιών 6DoF για μόνο πέντε λεπτά, είχε ως αποτέλεσμα την ταυτοποίησή τους κατά 95%[275]. Ο ΓΚΠΔ, εν προκειμένω, αρκείται στην *αδιαμφισβήτητη* ταυτοποίηση του χρήστη, χωρίς να διακρίνει μεταξύ άμεσης και έμμεσης. Επομένως, και αυτά τα δεδομένα τα οποία μπορούν εμμέσως να εξακριβώσουν την ταυτότητά του, θα εμπίπτουν στις οικείες προστατευτικές διατάξεις για τα βιομετρικά δεδομένα. Το ερώτημα που τίθεται είναι σε τι ποσοστό ακριβείας αρκείται ο ΓΚΠΔ, για να θεωρηθεί ότι πράγματι ταυτοποιούν αδιαμφισβήτητα το χρήστη (είναι αρκετό, άραγε, το 60%;). Όπως εκτιμάται, όμως, αρκεί η εύλογη πιθανολόγηση *("reasonable possibility")* ότι μέσω αυτών των δεδομένων θα υπάρξει ταυτοποίηση[276]. Προς αποφυγή καταστρατηγήσεων, θα ήταν σκόπιμο να δοθεί ρυθμιστική καθοδήγηση (regulatory guidance) για τη σαφή υπαγωγή στην έννοια των βιομετρικών και των εν λόγω δεδομένων που θα εξάγονται στο Metaverse.

(β) Βιομετρικού τύπου δεδομένα (biometrically-derived data): Ο ειδικός εξοπλισμός εμβύθισης στο Metaverse κατ' εξοχήν θα συγκεντρώνει, αποθηκεύει και επιτρέπει την επεξεργασία βιομετρικού τύπου δεδομένων που δεν θα καθιστούν (κατ' αρχήν) εφικτή την εξακρίβωση της ταυτότητας του χρήστη εν στενή εννοία, αλλά την ταυτοποίηση του πνευματικού και ψυχολογικού προφίλ του, δηλαδή την εξαγωγή συμπερασμάτων για τις συμπάθειες, αντιπάθειες, προτιμήσεις, επιθυμίες, τα ενδιαφέροντα, συναισθήματα, τους φόβους του κ.ο.κ. Τέτοια δεδομένα θα συλλέγονται, κατά πρώτον, για τη ρεαλιστική εμβύθιση του χρήστη στην πλατφόρμα, μέσω τεχνολογιών εντοπισμού της κίνησης των ματιών και των εκφράσεων του προσώπου-eye/face tracking, αλλά και της συνδυαστικά χρησιμοποιούμενης απτικής τεχνολογίας ή των διεπαφών BCI[277]. Μεταξύ αυτών συγκαταλέγονται οι κινήσεις των ματιών και της κόρης, η κατεύθυνση του βλέμματος[278], οι εκφράσεις του προσώπου, ο καρδιακός παλμός[279], η αρτηριακή πίεση, ο ρυθμός αναπνοής, η θερμοκρασία του σώματος[280], ο βαθμός εφίδρωσης, ακόμη και το μοτίβο των

[274] Ό.π., Kim, Y. (2022), σ. 237.

[275] Miller, M.R. et al. (2020) 'Personal identifiability of user tracking data during observation of 360-degree VR video', *Scientific Reports*, 10 (17404). Διαθέσιμο στο: https://doi.org/10.1038/s41598-020-74486-y.

[276] Ό.π., Kim, Y. (2022), σ. 243.

[277] Ό.π., Anidjar, L.Y., Packin, N.G. and Panezi, A. (2023), σ. 19.

[278] Ό.π., Martin, B. (2022), σ. 253.

[279] Ό.π., Anidjar, L.Y., Packin, N.G. and Panezi, A. (2023).

[280] Ό.π., Aamir, O. (2022), σ. 22.

εγκεφαλικών κυττάρων του χρήστη κ.ο.κ. Χαρακτηριστικά, το μοντέλο Quest Pro της Meta Platforms διαθέτει πέντε κάμερες με κατεύθυνση προς τα μέσα, οι οποίες καταγράφουν το πρόσωπο του χρήστη, επιτρέποντας στα άβαταρ, μεταξύ άλλων, να χαμογελάσουν, να κλείσουν το μάτι και να σηκώσουν το φρύδι τους[281]. Όλα αυτά τα δεδομένα θα υπόκεινται, όμως, σε περαιτέρω επεξεργασία από τους παρόχους που θα δραστηριοποιούνται στο Metaverse, και σε συνδυασμό με το ερέθισμα (stimuli) που προκάλεσε την εκάστοτε βιολογική αντίδραση, θα τους χαρίζουν πολύτιμες πληροφορίες για τον ψυχισμό των χρηστών, επιτρέποντάς τους να στοχεύουν τους τελευταίους με απόλυτα εξατομικευμένο (διαφημιστικό ή μη) περιεχόμενο. Η Brittan Heller περιγράφει το φαινόμενο της επεξεργασίας βιομετρικού τύπου δεδομένων για την προβολή στοχευμένων διαφημίσεων με τον όρο «βιομετρική ψυχογραφία» (biometric psychography)[282]. Μάλιστα, έρευνες έδειξαν ότι μόνο η ανάλυση δεδομένων από τεχνολογίες εντοπισμού της κίνησης των ματιών μπορεί να αποκαλύψει πληροφορίες για «*τη βιομετρική ταυτότητα, το φύλο, την ηλικία, την εθνικότητα, το σωματικό βάρος, τα χαρακτηριστικά της προσωπικότητας, τις συνήθειες κατανάλωσης ναρκωτικών, τη συναισθηματική κατάσταση, τις δεξιότητες και ικανότητες, τους φόβους, τα ενδιαφέροντα και τις σεξουαλικές προτιμήσεις του χρήστη*» ή να χρησιμοποιηθούν αυτές «*για τη διάγνωση διαφόρων σωματικών και ψυχικών παθήσεων*»[283]. Για παράδειγμα, αποδείχθηκε ότι οι ανεπαίσθητες κινήσεις των ματιών διαφοροποιούνται, όταν οι χρήστες αντικρίζουν ανθρώπους της ίδιας εθνικότητας συγκριτικά με άλλους[284]. Σε ορισμένες περιπτώσεις, βρέθηκε πως μόνο τρία δευτερόλεπτα ήταν αρκετός χρόνος, ώστε οι ως άνω τεχνολογίες να προβλέψουν σε ικανοποιητικό βαθμό ανθρώπινες αποφάσεις[285]. Ωστόσο, ο ΓΚΠΔ σωπαίνει σχετικά με αυτές τις κατηγορίες δεδομένων, η ειδική τεχνική

---

[281] Ό.π., Anidjar, L.Y., Packin, N.G. and Panezi, A. (2023).

[282] Heller, B. (2020) 'Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psychography, and the Law', *Vanderbilt Journal of Entertainment & Technology Law*, 23(1), σ. 1-51. Διαθέσιμο στο: https://scholarship.law.vanderbilt.edu/cgi/viewcontent.cgi?article=1000&context=jetlaw, σ. 27.

[283] Kröger, J.L., Lutz, O. and Müller, F. (2019) 'What Does Your Gaze Reveal About You? On the Privacy Implications of Eye Tracking', *Springer Link*. Διαθέσιμο στο: https://link.springer.com/chapter/10.1007/978-3-030-42504-3_15.

[284] Selinger, E., Altman, E. and Foster, S. (2023) 'Eye-Tracking in Virtual Reality A Visceral Notice Approach for Protecting Privacy', *Privacy Studies Journal*, 2, σ. 1–34. Διαθέσιμο στο: https://doi:10.7146/psj.v2i.134656, σ. 8.

[285] Common Sense (n.d.) 'Kids and the Metaverse: What Parents, Policymakers, and Companies Need to Know'. Διαθέσιμο στο: https://www.commonsensemedia.org/sites/default/files/featured-content/files/metaverse-white-paper.pdf, σ. 7.

επεξεργασία των οποίων δεν οδηγεί (κατ' αρχήν) σε αδιαμφισβήτητη ταυτοποίηση του υποκειμένου εν στενή εννοία, αλλά σε λεπτομερή κατάρτιση του ψυχογραφικού προφίλ του, δημιουργώντας έτσι ένα νομοθετικό κενό (loophole) που με μεγάλη άνεση θα σπεύσουν να εκμεταλλευτούν οι οικείοι πάροχοι στο Metaverse[286], για να επεξεργάζονται τέτοιου είδους βιομετρικές πληροφορίες χωρίς τις αυξημένες απαιτήσεις προστασίας που θέτει το άρθρο 9 παρ. 1 ΓΚΠΔ.

4. Συμπεριφορικά δεδομένα (behavioral data): Τα βιομετρικά δεδομένα του χρήστη που θα εξάγονται από τον ως άνω εξοπλισμό, θα μεταδίδονται στην εικονική πλατφόρμα σε πραγματικό χρόνο. Με αυτόν τον τρόπο, το άβαταρ θα αντικατοπτρίζει τις επιλογές, τις συνήθειες και τη συνολική συμπεριφορά του χρήστη εντός του Metaverse, φανερώνοντας τις πράξεις, τις προθέσεις και τις νοητικές διεργασίες του[287]. Παράλληλα, θα αποκαλύπτει τον τρόπο με τον οποίο ο χρήστης αλληλεπιδρά με το περιβάλλον του και επικοινωνεί με τους υπόλοιπους χρήστες, είτε αυτή η επικοινωνία είναι προφορική, είτε γραπτή, είτε μη λεκτική[288]. Τουτέστιν, η δραστηριότητα του άβαταρ στο εικονικό περιβάλλον θα μπορεί να οδηγήσει στην εξαγωγή απλών[289] και ευαίσθητων[290] προσωπικών δεδομένων του χρήστη, αλλά και πολύτιμων συμπερασμάτων για το πνευματικό και ψυχολογικό προφίλ του[291], τα οποία οι οικείοι πάροχοι πάλι θα αξιοποιούν για ίδια συμφέροντα.

Τα ανωτέρω οδηγούν με μαθηματική ακρίβεια στο συμπέρασμα ότι τα υποκείμενα στο Metaverse θα βρίσκονται υπό συνεχή παρακολούθηση, εκθέτοντας μαζικά και σε κοινή θέα ιδίως ευαίσθητα προσωπικά τους δεδομένα, που θα συλλέγονται και θα αξιοποιούνται για διάφορους σκοπούς· για την εξατομίκευση του διαμοιραζόμενου περιεχομένου (tailored content) και τη στοχευόμενη, συμπεριφορική διαφήμιση (behavioral advertising), για την αυτοματοποιημένη λήψη αποφάσεων (automated-decision making)[292], μεταξύ των οποίων η σκιαγράφηση άκρως παρεμβατικών για την ιδιωτικότητα προφίλ (deep profiling)[293], για

---

[286] Ό.π., Aamir, O. (2022), σ. 6.

[287] Ό.π., Anidjar, L.Y., Packin, N.G. and Panezi, A. (2023), σ. 20.

[288] Ό.π., σ. 21.

[289] Για παράδειγμα, οι δραστηριότητες του άβαταρ και τα εικονικά μέρη που συχνάζει, θα μπορούν να αποκαλύψουν την πραγματική ηλικία του χρήστη, ακόμη κι αν αυτός την έχει αποκρύψει.

[290] Για παράδειγμα, η παρεύρεση του άβαταρ σε πολιτικές ομιλίες και εκδηλώσεις θα μπορεί να αποκαλύψει τα πολιτικά πιστεύω του χρήστη.

[291] Πχ. πόσο παρορμητικός είναι ή ευεπίφορος σε καταχρήσεις.

[292] Ό.π., Knibbeler, D., Mohrmann, M. and Zadeh, S. (2022).

[293] European Data Protection Supervisor (2023) *Metaverse.* Διαθέσιμο στο: https://edps.europa.eu/press-publications/publications/techsonar/metaverse_en [Πρόσβαση 23 Μαΐου 2023].

σκοπούς κρατικής εποπτείας (state surveillance)[294], επηρεασμού της ψήφου κι εν γένει πολιτικής χειραγώγησης κ.ο.κ. Αναντίλεκτα, χωρίς ισχυρές εγγυήσεις περί ιδιωτικότητας, το Metaverse θα αποτελέσει γόνιμο έδαφος για ακραία εκμετάλλευση και συστηματική παραβίαση θεμελιωδών ανθρώπινων δικαιωμάτων και ελευθεριών.

Στο πλαίσιο αυτό, θα πρέπει πρώτα απ' όλα να δοθεί νομοθετική λύση, ώστε να συμπεριληφθούν ρητώς στην κατηγορία των ευαίσθητων βιομετρικών δεδομένων των άρθρων 9 παρ. 1 και 4 παρ. 14 ΓΚΠΔ, εκείνες οι βιομετρικού τύπου πληροφορίες που θα μπορούν πλέον – και πράγματι, θα χρησιμοποιούνται *με σκοπό*- να ταυτοποιήσουν με ακρίβεια το ψυχογραφικό προφίλ του υποκειμένου[295]. Η συλλογή των πληροφοριών αυτών είναι αδύνατον μέχρι αυτή τη στιγμή να οδηγήσει σε τέτοια ταυτοποίηση, αφενός, γιατί είναι περιορισμένη σε έκταση και αφετέρου, γιατί δεν εφαρμόζεται στο πλαίσιο ολοκληρωμένων εικονικών κόσμων, όπως το Metaverse. Έτσι, ένα έξυπνο ρολόι (smartwatch) μπορεί σήμερα να μετρήσει τους καρδιακούς παλμούς μας, αλλά δεν μπορεί να γνωρίζει ποιο εξωτερικό ερέθισμα πυροδότησε την αύξησή τους. Αντίθετα, ο χρήστης θα εισέρχεται στο Metaverse εξοπλισμένος με μηχανισμούς που θα καταγράφουν κάθε βιολογική αντίδραση που θα συμβαίνει στο σώμα του, κάθε ανεπαίσθητη κίνηση των μυών και των μελών του και κάθε συστολή ή διαστολή της κόρης των ματιών του, για να ζήσει μια παράλληλη εικονική ζωή, σκηνοθετημένη με τρόπο που να αντιγράφει κατά γράμμα τις εμπειρίες και τα ερεθίσματα της πραγματικής. Κατά συνέπεια, οι χρήστες στο Metaverse θα είναι απόλυτα *«διαφανείς» (transparent)*[296], με αποτέλεσμα οι πάροχοι να έχουν σχεδόν τη δύναμη να διαβάζουν το μυαλό τους. Αναμφίβολα, λοιπόν, η επεξεργασία των ως άνω βιομετρικών πληροφοριών θα πρέπει να περιβάλλεται με τα αυξημένα εχέγγυα προστασίας του άρθρου 9 ΓΚΠΔ, για την αποτελεσματική προστασία της ιδιωτικότητας των χρηστών.

Περαιτέρω, αυτό που πρέπει να διερευνηθεί εγκαίρως από τις ρυθμιστικές και εποπτικές αρχές, είναι το αν (και πώς) αυτή η ευρεία και μαζική συλλογή προσωπικών δεδομένων που θα συντελείται στο Metaverse, μπορεί να συμμορφώνεται προς τις αρχές επεξεργασίας που θεσπίζει ο ΓΚΠΔ στο άρθρο 5 παρ. 1 αυτού, και ειδικότερα, προς τις

---

[294] Ό.π., European Parliamentary Research Service (EPRS) (2022), σ. 5.

[295] Βλ. ό.π., Dick, E. (2021), σ. 21 και Martin, B. (2022), σ. 259.

[296] Ό.π., Kalpokas, I. and Kalpokienė, J. (2023), σ. 21.

αρχές ελαχιστοποίησης των δεδομένων, περιορισμού του σκοπού και περιορισμού της περιόδου αποθήκευσής τους.

Ειδικότερα, η αρχή της ελαχιστοποίησης των δεδομένων (data minimization) του άρθρου 5 παρ. 1 στοιχ. γ' ΓΚΠΔ, επιβάλλει την επεξεργασία μόνο όσων προσωπικών δεδομένων κρίνονται κατάλληλα, συναφή και αναγκαία για τους σκοπούς της εκάστοτε επεξεργασίας. Η αρχή του περιορισμού του σκοπού (purpose limitation) του άρθρου 5 παρ. 1 στοιχ. β' ΓΚΠΔ, ορίζει ότι τα δεδομένα πρέπει να συλλέγονται μόνο για νόμιμους, καθορισμένους και ρητούς σκοπούς και ότι δεν πρέπει να υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους εν λόγω σκοπούς, ενώ σύμφωνα με τη Γνώμη 3/2013 της Ομάδας προστασίας δεδομένων του άρθρου 29, ο κάθε σκοπός πρέπει να είναι σαφώς και ειδικώς προσδιορισμένος και αρκετά λεπτομερής, ώστε να μπορεί να προσδιοριστεί το είδος της επεξεργασίας που περιλαμβάνεται ή δεν περιλαμβάνεται σε αυτόν[297]. Η αρχή του περιορισμού της περιόδου αποθήκευσης (storage limitation) του άρθρου 5 παρ. 1 στοιχ. ε' ΓΚΠΔ, θεσπίζει ότι τα δεδομένα πρέπει να διατηρούνται σε μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα που απαιτείται για την επίτευξη των σκοπών της επεξεργασίας.

Το Metaverse μοιάζει *εγγενώς αντίθετο* προς τις αρχές αυτές. Από την ανωτέρω ανάλυση προκύπτει ότι η επεξεργασία άπειρων προσωπικών δεδομένων των χρηστών θα αναχθεί σε αναγκαία συνθήκη για τη λειτουργία του και την αληθοφανή εμβύθισή τους στον εικονικό κόσμο[298]. Παράλληλα, η επεξεργασία θα συντελείται για την εξατομίκευση του προβαλλόμενου περιεχομένου. Εντούτοις, ο λεπτομερής προσδιορισμός όλων των ειδικότερων σκοπών που εμπίπτουν στην ευρύτερη έννοια της εξατομίκευσης, θα είναι εκ των πραγμάτων αδύνατος σε ένα οικοσύστημα που υπόσχεται την πλήρη και συνεχή προσαρμογή της εικονικής εμπειρίας και των επιμέρους υπηρεσιών στην προσωπικότητα κάθε χρήστη[299]. Τέλος, από τη στιγμή που η ζωή στο Metaverse θα κυλάει παράλληλα με τη ζωή στη Γη, χωρίς να μπορεί να τερματίσει, αμφισβητείται έντονα το κατά πόσο θα μπορεί να περιοριστεί το χρονικό διάστημα αποθήκευσης των προσωπικών δεδομένων σε μορφή

---

[297] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, της 2ας Απριλίου 2013. Διαθέσιμο στο: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

[298] Ό.π., Anidjar, L.Y., Packin, N.G. and Panezi, A. (2023), σ. 18.

[299] Βλ. ό.π., Kim, Y. (2022), σ. 246, για την αδυναμία εξαντλητικού καθορισμού όλων των ειδικότερων σκοπών που εμπίπτουν στην έννοια της εξατομίκευσης στο περιβάλλον VR/AR.

που να επιτρέπει την ταυτοποίηση των χρηστών, όσο αυτοί δεν αποσυνδέονται οριστικά από την εκάστοτε πλατφόρμα, αλλά συνεχίζουν να κάνουν χρήση των παρεχόμενων υπηρεσιών της[300].

Ωστόσο, η όποια προσπάθεια απόκρυψης, ανωνυμοποίησης ή περιορισμού της πρόσβασης σε τέτοιου είδους δεδομένα θα αποστερήσει από την εικονική εμπειρία αυτό που υπόσχεται ότι θα προσφέρει, καθιστώντας την ύπαρξη των οικείων πλατφορμών ουσιαστικά αλυσιτελή και εμποδίζοντας την τεχνολογική πρόοδο και την καινοτομία[301]. Γι' αυτό το λόγο, είναι καίριο να βρεθούν οι κατάλληλες ισορροπίες μεταξύ της ανάγκης προστασίας του δικαιώματος στα προσωπικά δεδομένα και της λειτουργικότητας των εικονικών πλατφορμών Metaverse[302], ως προϊόντων, αλλά και παραγόντων τεχνολογικής ακμής.

Κατά συνέπεια, θα πρέπει οπωσδήποτε να διερευνηθεί από τις ρυθμιστικές και εποπτικές αρχές ποια προσωπικά δεδομένα κρίνονται ως *απολύτως αναγκαία* και σε συνάρτηση με *ποιους σκοπούς* για την *ουσιαστική* λειτουργία του Metaverse (πχ. κρίνεται απαραίτητη η εξαντλητική καταγραφή των κινήσεων των ματιών και των εκφράσεων του προσώπου του χρήστη για τη ρεαλιστική εμβύθισή του[303] ή των εγκεφαλικών σημάτων του για την εξατομίκευση του προβαλλόμενου περιεχομένου;), ώστε να μην υπόκεινται σε επεξεργασία από τους οικείους παρόχους μη αναγκαία προσωπικά δεδομένα του χρήστη, ενώ από την άλλη πλευρά, θα πρέπει να ληφθεί μέριμνα για την ελαχιστοποίηση της καταγραφής και περαιτέρω επεξεργασίας προσωπικών δεδομένων τρίτων προσώπων[304], τα οποία ενδέχεται να βρίσκονται πλησίον του χρήστη της ειδικής διεπαφής, αγνοώντας τους κινδύνους για την ιδιωτικότητά τους. Το πιο σημαντικό, όμως, είναι να καθιερωθεί ένα διαφανές εικονικό περιβάλλον, στο οποίο οι χρήστες θα ενημερώνονται ουσιωδώς για τη φύση, τους σκοπούς και τα όρια των επιμέρους πράξεων επεξεργασίας και θα μπορούν να

---

[300] Βλ. ό.π., Dick, E. (2021), σ. 16, για τη δυσκολία ουσιαστικής ανωνυμοποίησης των δεδομένων σε ένα περιβάλλον όπου η επαναταυτοποίηση των υποκειμένων θα είναι μονίμως δυνατή, χάρη στη βιομετρική ανάλυση των (μοναδικών) κινήσεών τους.

[301] Ό.π., Dick, E. (2021), σ. 9.

[302] Βλ. Dick, E. (2021), σ. 24, για VR/AR.

[303] Schlemann, D. (2022) 'Metaverse Blog Series: No. 5 – Data Privacy in the Metaverse', *Arqis*, 28 Οκτωβρίου. Διαθέσιμο στο: https://www.arqis.com/en/blogs/metaverse-blog-5-data-privacy-in-the-metaverse/ [Πρόσβαση 23 Μαΐου 2023].

[304] Πχ. μέσω περιορισμού του οπτικού πεδίου των ειδικών συσκευών εμβύθισης, ενσωμάτωσης σε αυτές φίλτρων θόλωσης εικόνας, τοπικής μόνο αποθήκευσης των όποιων συλλεγέντων δεδομένων κ.ο.κ.

επιλέγουν αυτόνομα ποια προσωπικά δεδομένα τους επιθυμούν να αποκαλύψουν, σε ποιους και για ποιους - μη αναγκαίους για τη λειτουργία του Metaverse - σκοπούς.

Σε κάθε περίπτωση, το άρθρο 25 ΓΚΠΔ επιτάσσει στους υπεύθυνους επεξεργασίας να λαμβάνουν κατάλληλα τεχνικά και οργανωτικά μέτρα (πχ. κρυπτογράφηση, ψευδωνυμοποίηση κ.ά.) για να συμμορφώνονται προς τις αρχές προστασίας προσωπικών δεδομένων ήδη από το σχεδιασμό (by design), δηλαδή κατά την ανάπτυξη κάθε νέας τεχνολογίας, αλλά και εξ ορισμού (by default), δηλαδή με τρόπο, ώστε να μην απαιτείται η παρέμβαση του φυσικού προσώπου για να διασφαλίσει την προστασία (πχ. καθιέρωση ενός συστήματος opt-in και όχι opt-out για να καταστούν προσβάσιμα τα δεδομένα σε αόριστο αριθμό προσώπων). Το ίδιο θα πρέπει να πράξουν, επομένως, και οι υπεύθυνοι επεξεργασίας στο Metaverse. Η εκτίμηση αντικτύπου (Data Protection Impact Assessment/DPIA) που προβλέπεται στο άρθρο 35 ΓΚΠΔ, αποτελεί ουσιαστικό εργαλείο για την προστασία της ιδιωτικότητας των υποκειμένων και θα πρέπει ομοίως να διενεργείται από τους υπευθύνους επεξεργασίας στο Metaverse[305], για την εκ των προτέρων αξιολόγηση των επιπτώσεων των σχεδιαζόμενων από αυτούς πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα, λόγω του υψηλού κινδύνου που ενδέχεται να εγκυμονεί το Metaverse για τα δικαιώματα και τις ελευθερίες των χρηστών και των γύρω τους[306]. Τέλος, η τήρηση εγκεκριμένων κωδίκων δεοντολογίας (άρθρο 40 ΓΚΠΔ) και μηχανισμών πιστοποίησης (άρθρο 42 ΓΚΠΔ) από τους οικείους υπεύθυνους επεξεργασίας, θα λαμβάνεται δεόντως υπόψη για την αξιολόγηση της συμμόρφωσής τους προς τον ΓΚΠΔ.

3.2. Κατανομή ρόλων μεταξύ των συμμετεχόντων μερών

Ένα από τα πλέον ακανθώδη ζητήματα το οποίο θα απασχολήσει κατά κόρον το νομοθετικό σώμα, τις εποπτικές αρχές, αλλά και σύσσωμο τον επιχειρηματικό κόσμο που θα δραστηριοποιηθεί στο χώρο του Metaverse, θα προκαλέσει, δε, τριγμούς στην αποτελεσματική εφαρμογή του ΓΚΠΔ στο εικονικό περιβάλλον, είναι ο σαφής

[305] Βλ. Kim, Y. (2022), σ. 245 για Dpias σε περιβάλλοντα Εικονικής Πραγματικότητας.

[306] Βλ. άρθρο 35 παρ. 3 ΓΚΠΔ, σύμφωνα με το οποίο η εκτίμηση αντικτύπου απαιτείται ιδίως σε περίπτωση (α) «*συστηματικής και εκτενούς αξιολόγησης προσωπικών πτυχών σχετικά με φυσικά πρόσωπα, η οποία βασίζεται σε αυτοματοποιημένη επεξεργασία, περιλαμβανομένης της κατάρτισης προφίλ, και στην οποία βασίζονται αποφάσεις που παράγουν έννομα αποτελέσματα σχετικά με το φυσικό πρόσωπο ή ομοίως επηρεάζουν σημαντικά το φυσικό πρόσωπο*» και (β) «*μεγάλης κλίμακας επεξεργασίας των ειδικών κατηγοριών δεδομένων που αναφέρονται στο άρθρο 9 παράγραφος 1*».

προσδιορισμός των ρόλων και η κατανομή των αντίστοιχων υποχρεώσεων και ευθυνών μεταξύ της σωρείας συμμετεχόντων στη σχετική αγορά[307].

Σύμφωνα με την αρχή της λογοδοσίας (accountability)[308], οι υπεύθυνοι επεξεργασίας (data controllers) φέρουν το βάρος απόδειξης και την ευθύνη συμμόρφωσης στις διατάξεις του ΓΚΠΔ, ενώ ταυτόχρονα, είναι τα πρόσωπα εκείνα έναντι των οποίων τα υποκείμενα νομιμοποιούνται να ασκούν τα δικαιώματά τους δυνάμει του ΓΚΠΔ. Στο πλαίσιο των αρμοδιοτήτων τους εμπίπτει, μεταξύ άλλων, η παροχή οδηγιών και η άσκηση εποπτείας[309] επί των εκτελούντων (data processors), στους οποίους έχουν τυχόν αναθέσει την επεξεργασία των δεδομένων, προκειμένου να διασφαλιστεί το σύννομο των ενεργειών των τελευταίων. Οι εκτελούντες, από την άλλη, έχουν περιορισμένες - αλλά ουσιώδεις - υποχρεώσεις δυνάμει του ΓΚΠΔ και ενεργούν μόνο κατ' εντολή των υπευθύνων[310]. Αν, παρά ταύτα, υπερβούν τις εντολές αυτές, θεωρούνται υπεύθυνοι ως προς την επίμαχη επεξεργασία, ενώ ενδέχεται να υποστούν κυρώσεις για τη σχετική υπέρβαση[311].

Ειδικότερα, το άρθρο 4 στοιχ. 7 ΓΚΠΔ ορίζει ως «υπεύθυνο επεξεργασίας» το «*φυσικό ή νομικό πρόσωπο, τη δημόσια αρχή, την υπηρεσία ή άλλο φορέα που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα*», ενώ το άρθρο 4 στοιχ. 8 ΓΚΠΔ ορίζει ως «εκτελούντα την επεξεργασία» το «*φυσικό ή νομικό πρόσωπο, τη δημόσια αρχή, την υπηρεσία ή άλλο φορέα που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας*». Το δε άρθρο 26 παρ. 1 ΓΚΠΔ αναγνωρίζει ως από «κοινού υπεύθυνους επεξεργασίας» (joint controllers) δύο ή περισσότερους υπεύθυνους που «*καθορίζουν από κοινού τους σκοπούς και τα μέσα της επεξεργασίας*».

Η ιδιότητα του υπευθύνου επεξεργασίας απονέμεται σε συνάρτηση με την εκάστοτε πραγματοποιούμενη επεξεργασία και εξαρτάται μόνο από το πραγματικό υπόβαθρο κάθε περίπτωσης (case-by-case analysis) και όχι από την τυπική υπόδειξη ενός υπευθύνου σε ένα

---

[307] Ό.π., Καρδαμάκη, Α. (2022) και ό.π., Κοντογεώργου, Π., Συρμακέζη, Ζ., Ζούλοβιτς, Μ. (2022), σ. 54.

[308] Βλ. άρθρο 5 παρ. 2 σε συνδυασμό με τα άρθρα 24 και 32 ΓΚΠΔ.

[309] Βλ. άρθρο 29 ΓΚΠΔ.

[310] Ό.π.

[311] Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, Κατευθυντήριες γραμμές 07/2020 σχετικά με τις έννοιες του υπευθύνου επεξεργασίας και του εκτελούντος την επεξεργασία στον ΓΚΠΔ, Έκδοση 2.0, της 7ης Ιουλίου 2021. Διαθέσιμο στο: https://edpb.europa.eu/system/files/2022-02/eppb_guidelines_202007_controllerprocessor_final_el.pdf, σ. 4.

νομικό έγγραφο (πχ. στους Όρους Παροχής Υπηρεσιών)[312]. Σύμφωνα, λοιπόν, με την Ομάδα προστασίας δεδομένων του άρθρου 29, ο καθορισμός του σκοπού και των μέσων της επεξεργασίας αντιστοιχεί στο *γιατί* (ποιο είναι το κίνητρο[313] για την επεξεργασία;) και το *πώς* (πχ. ποια είναι τα τεχνικά και οργανωτικά μέτρα[314] που χρησιμοποιούνται για την επεξεργασία;) τα δεδομένα υπόκεινται σε επεξεργασία και άρα, η ευθύνη απονέμεται σε όποιον έχει αποφασιστική επιρροή στον εν λόγω καθορισμό[315].

Περαιτέρω, ενώ ο ΓΚΠΔ ρυθμίζει ως ισάξιας σπουδαιότητας τον σκοπό και τα μέσα της επεξεργασίας για την απονομή της ιδιότητας του υπευθύνου, τόσο η νομολογία όσο και οι Κατευθυντήριες γραμμές των εποπτικών αρχών δίνουν προβάδισμα στον σκοπό αυτής, υπό την έννοια ότι ο καθορισμός του σκοπού επισύρει άνευ άλλου τινός την εφαρμογή του ΓΚΠΔ, ενώ το ίδιο δεν συμβαίνει με τον καθορισμό απλώς των (τεχνικών και οργανωτικών) μέσων της επεξεργασίας[316]. Έτσι, είναι δυνατόν ο υπεύθυνος να καθορίζει μόνο το σκοπό, ενώ ο εκτελών αποκλειστικά τα (τεχνικά και οργανωτικά) μέσα της επεξεργασίας[317]. Ωστόσο, στην έννοια των μέσων συγκαταλέγονται και μέσα ουσιώδους σημασίας *("effective means")*, ο καθορισμός των οποίων ανήκει εγγενώς στον υπεύθυνο, όπως το ποια δεδομένα θα τύχουν επεξεργασίας, για πόσο καιρό θα υπόκεινται σε αυτήν, ποιος θα έχει πρόσβαση στα δεδομένα κ.ο.κ[318].

Η σημασία του σαφούς καθορισμού του υπευθύνου είναι αδιαπραγμάτευτη για την ουσιαστική εφαρμογή του ΓΚΠΔ. Το ΔΕΕ, στην υπόθεση Google Spain, υπογράμμισε την ανάγκη για μια ευρεία ερμηνεία του όρου, ώστε να διασφαλιστεί η αποτελεσματική και πλήρης προστασία των υποκειμένων[319].

Ωστόσο, στο αχανές οικοσύστημα του Metaverse, ο ακριβής προσδιορισμός των υπευθύνων και των από κοινού υπευθύνων, αλλά και ο διαχωρισμός αυτών από τους

---

[312] Ό.π., Panel for the Future of Science and Technology (STOA) (2019), σ. 37.

[313] Πχ. η απευθείας εμπορική προώθηση.

[314] Πχ. το Blockchain, το κέντρο δεδομένων (data center) που θα χρησιμοποιηθεί κ.ο.κ.

[315] Ό.π., Κατευθυντήριες γραμμές 7/2020, σ. 15.

[316] Ό.π., Panel for the Future of Science and Technology (STOA) (2019), σ. 39.

[317] Ό.π.

[318] Ό.π., Κατευθυντήριες γραμμές 7/2020, σ. 17.

[319] Απόφαση ΔΕΕ C-131/12, Google Spain, της 13ης Μαΐου 2014. Διαθέσιμο στο: https://curia.europa.eu/juris/document/document.jsf;jsessionid=4415E5F4881AE4B87EB3474981CBECBF?text=&docid=152065&pageIndex=0&doclang=el&mode=lst&dir=&occ=first&part=1&cid=18541420, αιτιολογική σκέψη 38.

εκτελούντες, αναμένεται να αποδειχθεί ιδιαίτερη απαιτητική διαδικασία[320]. Παρακάτω, θα επιχειρήσουμε να προσδιορίσουμε σχηματικά τα υπόχρεα μέρη στο Metaverse, ανάλογα με τα (λιγότερο ή περισσότερο) πιθανά σενάρια διαμόρφωσης του οικοσυστήματός του. Ειδικότερα:

Στην περίπτωση που μία κεντρική οντότητα ελέγχει και διαχειρίζεται ολόκληρο το Metaverse, καθορίζοντας κατ' αποκλειστικότητα *γιατί* (θα προβαίνει σε καθορισμό των σκοπών της επεξεργασίας, πχ. της προβολής διαφημίσεων) και *πώς* (θα παρέχει την πλατφόρμα Metaverse και όλα τα βασικά εργαλεία για τη διαχείριση χρηστών, πχ. την εγγραφή και διαγραφή λογαριασμών[321]) τα προσωπικά δεδομένα των χρηστών υπόκεινται σε επεξεργασία, τότε η εν λόγω κεντρική οντότητα θα λειτουργεί υπό την ιδιότητα του υπευθύνου επεξεργασίας και τυχόν τρίτα μέρη παροχής υπηρεσιών, όπως ανάλυσης αποτελεσμάτων (analytics), ελέγχου ασφάλειας λογαριασμών (account security), διαφήμισης (promotion) κλπ., που θα επεξεργάζονται δεδομένα μόνο για λογαριασμό της, θα λειτουργούν ως εκτελούντες[322].

Αντιθέτως, στην πλέον πιθανή περίπτωση που στην επεξεργασία των προσωπικών δεδομένων των χρηστών συμμετέχουν για ίδιους σκοπούς (εμπορικούς/επιχειρηματικούς, επαγγελματικούς, πολιτικούς κ.ά.) περισσότερα φυσικά ή νομικά πρόσωπα, δημόσιες αρχές, υπηρεσίες και φορείς, ασκώντας με αυτόν τον τρόπο αποφασιστική επιρροή και στα μέσα της επεξεργασίας, τότε κάθε τέτοιο πρόσωπο θα χαρακτηρίζεται ως υπεύθυνος επεξεργασίας υπό την έννοια του ΓΚΠΔ. Έτσι, ως υπεύθυνοι επεξεργασίας θα θεωρούνται τόσο ο πάροχος της εικονικής πλατφόρμας και ο προμηθευτής του ειδικού εξοπλισμού εμβύθισης, όσο και κάθε χρήστης[323] που θα προσφέρει ή διαφημίζει αγαθά ή υπηρεσίες εντός του Metaverse (πχ. έμποροι - marketers, διαφημιστές – advertisers κ.ά.) ή κατ' άλλο τρόπο συμμετέχει σε αυτό (πχ. πολιτικά κόμματα για την ενίσχυση προεκλογικής καμπάνιας, εργοδότες για την πρόσληψη εργαζομένων κ.ά.) και επεξεργάζεται γι' αυτό το

---

320 Ό.π., European Parliamentary Research Service (EPRS) (2022), σ. 5.

321 Kosta, E. et al. (2010) 'Data protection issues pertaining to social networking under EU law', *Transforming Government: People, Process and Policy*, 4(2), σ. 193–201. Διαθέσιμο στο: https://doi.org/10.1108/17506161011047406, σ. 196.

322 Ongun, C.A. (2022) 'Turkey: Evaluation On The Concepts Of Data Controller And Data Processor In The Metaverse' *Mondaq*, 22 Δεκεμβρίου. Διαθέσιμο στο: https://www.mondaq.com/turkey/data-protection/1263864/evaluation-on-the-concepts-of-data-controller-and-data-processor-in-the-metaverse#_ftn27 [Πρόσβαση 6 Μαΐου 2023].

323 Ό.π., Καρδαμάκη, Α. (2022).

λόγο προσωπικά δεδομένα των χρηστών ή και παρακολουθεί τη συμπεριφορά τους. Μάλιστα, τα εν λόγω πρόσωπα ενδέχεται να θεωρηθούν από κοινού υπεύθυνοι επεξεργασίας κατά την έννοια του άρθρου 26 ΓΚΠΔ, υπό τον όρο ότι καθορίζουν από κοινού τους σκοπούς και τα μέσα της επεξεργασίας[324].

Εν προκειμένω, υποστηρίζεται[325] ότι μπορεί να εφαρμοστεί αναλογικά η νομολογία του ΔΕΕ[326], σύμφωνα με την οποία τόσο το Facebook, όσο και ο διαχειριστής ιστοσελίδας Fan Page στο Facebook, κρίθηκαν ως από κοινού υπεύθυνοι επεξεργασίας των προσωπικών δεδομένων των επισκεπτών της εν λόγω ιστοσελίδας. Πιο συγκεκριμένα, το Facebook, με σκοπό να βελτιώσει το σύστημα διαφημίσεών του, μοιραζόταν με τον εν λόγω διαχειριστή ανωνυμοποιημένα στατιστικά σχετικά με τα δημογραφικά και γεωγραφικά στοιχεία και τον τρόπο ζωής και τα ενδιαφέροντα των επισκεπτών της συγκεκριμένης ιστοσελίδας και ειδικότερα, του στοχευόμενου κοινού (target audience) της εν λόγω επιχείρησης. Αυτό καθίστατο δυνατό χάρη στην κατάρτιση κριτηρίων στόχευσης κοινού από το Facebook και στον επακόλουθο προσδιορισμό αυτών από το διαχειριστή της ιστοσελίδας, που εμπεριείχε αναγκαστικά και αίτημα προς το Facebook για την επεξεργασία των υπό κρίση δεδομένων, με σκοπό την αποτελεσματικότερη προώθηση των προσφερόμενων υπηρεσιών του διαχειριστή. Έτσι, κρίθηκε ότι ο τελευταίος, αν και δεν είχε ο ίδιος πρόσβαση στα προσωπικά δεδομένα των χρηστών, αλλά σε μια ανωνυμοποιημένη μορφή αυτών, είχε, παράλληλα με το Facebook, αποφασιστική επιρροή στη διαμόρφωση του σκοπού και των μέσων της επεξεργασίας, υπό την έννοια ότι οριοθετούσε τις παραμέτρους που καθόριζαν εντέλει τίνος τα προσωπικά δεδομένα θα τύχουν επεξεργασίας[327]. Ομοίως, η ως άνω απόφαση δέχθηκε ότι πρέπει να υιοθετηθεί μια ευρεία ερμηνεία του όρου «από κοινού υπεύθυνος επεξεργασίας», με σκοπό την πλήρη και αποτελεσματική προστασία των υποκειμένων[328].

---

[324] Ό.π., Schlemann, D. (2022).

[325] Lecocq, D. and Omer, L. M. (2022) 'The Privacy, Data Protection and Cybersecurity Law Review: Metaverse and the Law' *The Law Reviews*, 27 Οκτωβρίου. Διαθέσιμο στο: https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/metaverse-and-the-law [Πρόσβαση 6 Μαΐου 2023] και ό.π., Schlemann, D. (2022).

[326] Βλ. απόφαση ΔΕΕ C-210/16, Wirtschaftsakademie Schleswig-Holstein GmbH, της 5ης Ιουνίου 2018. Διαθέσιμο στο: https://curia.europa.eu/juris/document/document.jsf?text=&docid=202543&pageIndex=0&doclang=el&mode=lst&dir=&occ=first&part=1&cid=18623509.

[327] Ό.π., Κατευθυντήριες γραμμές 07/2020, σ. 21-22.

[328] Ό.π., απόφαση ΔΕΕ C-210/16, αιτιολογική σκέψη 23.

Κατ' αναλογία, τόσο ο πάροχος της πλατφόρμας Metaverse, όσο και ο διαχειριστής ενός εικονικού πολυκαταστήματος, αλλά και ο ιδιοκτήτης ενός εικονικού καταστήματος στεγαζόμενου εντός του, θα μπορούν, ενδεικτικά, να θεωρηθούν από κοινού υπεύθυνοι υπό την έννοια του άρθρου 26 ΓΚΠΔ[329], για την επεξεργασία των προσωπικών δεδομένων των επισκεπτών τους. Υπό τις ίδιες προϋποθέσεις, στο μέτρο, δηλαδή, που συγκαθορίζουν τους σκοπούς και τα μέσα της υπό κρίση επεξεργασίας, θα θεωρηθούν από κοινού υπεύθυνοι ο πάροχος της εικονικής πλατφόρμας και ο πάροχος της ειδικής συσκευής εμβύθισης στο Metaverse[330](αν δεν ταυτίζονται). Για τις πράξεις επεξεργασίας, βέβαια, το σκοπό και τα μέσα των οποίων καθορίζει κάθε υπεύθυνος ξεχωριστά, δεν θα υπάρχει συνευθύνη[331].

Από την άλλη, οι πάροχοι υπηρεσιών νεφοϋπολογιστικής (Cloud Service Providers), οι οποίοι κατ' αρχήν επεξεργάζονται δεδομένα προσωπικού χαρακτήρα των χρηστών μόνο για λογαριασμό και υπό τις οδηγίες και την εποπτεία των πελατών τους, όπως είναι οι πάροχοι υπηρεσιών Infrastructure-as-a-Service (Iaas), Platform-as-a-Service (Paas) και Software-as-a-Service (SaaS) ή εδώ, Metaverse-as-a-Service (MaaS), θα λειτουργούν ως εκτελούντες[332] [333]. Το ίδιο θα ισχύει και για κάθε τρίτο μέρος που θα επεξεργάζεται προσωπικά δεδομένα χρηστών μόνο για λογαριασμό των υπευθύνων (πχ. μεσίτες δεδομένων -data suppliers κ.ά). Όπως αναφέρθηκε ανωτέρω, ο τυχόν καθορισμός των τεχνικών και οργανωτικών μέσων δεν αρκεί από μόνος του για να προσδώσει στα οικεία πρόσωπα την ιδιότητα του υπευθύνου.

Ο προσδιορισμός των ρόλων των υπόχρεων μερών και κατ' επέκταση των συναφών υποχρεώσεων και ευθυνών τους θα πρέπει να λαμβάνει χώρα για κάθε επεξεργασία χωριστά. Εντούτοις, με δεδομένο ότι οι δραστηριοποιούμενες στο Metaverse οντότητες θα διασυνδέονται με δαιδαλώδεις σχέσεις και θα επεξεργάζονται διαρκώς, μαζικώς και με αυτοματοποιημένο τρόπο τα προσωπικά δεδομένα των χρηστών, είναι αυτονόητο ότι θα είναι εξαιρετικά επίπονο, αν όχι αδύνατον, να προσδιοριστεί με ακρίβεια και σαφήνεια ποιος κρύβεται πίσω από κάθε διενεργούμενη επεξεργασία, για λογαριασμό ποίου

[329] Ό.π., Schlemann, D. (2022).

[330] Ό.π., Καρδαμάκη, Α. (2022).

[331] Ό.π., Κατευθυντήριες γραμμές 07/2020, σ. 30.

[332] Ό.π., Ongun, C.A. (2022).

[333] Εκτός αν η επεξεργασία των δεδομένων πραγματοποιείται από αμφότερους για κοινούς σκοπούς (πχ. ασφάλεια), οπότε ενδέχεται να θεμελιώνεται από κοινού ευθύνη (βλ. Κουσουνή-Πανταζοπούλου, Α. (2022) *Cloud Computing & νομικά ζητήματα.* Αθήνα: Νομική Βιβλιοθήκη, σ. 155).

επεξεργάζεται τα δεδομένα[334] και ποιους σκοπούς υπηρετεί. Ελλείψει, όμως, μιας τέτοιας ασφαλούς κατανομής, θα είναι πρακτικά ανέφικτο να διασφαλιστεί η προστασία της ιδιωτικότητας των υποκειμένων στο Metaverse, με ό,τι αυτό συνεπάγεται για θεμελιώδη ανθρώπινα δικαιώματα και ελευθερίες και τελικά, για το ίδιο το μέλλον του εικονικού κόσμου.

Ενόψει των περιγραφόμενων προκλήσεων, είναι πολύ πιθανό η ορθή ανάγνωση της ενωσιακής νομοθεσίας να χρειαστεί ρυθμιστική καθοδήγηση σχετικά με τους συγκεκριμένους ρόλους των εμπλεκόμενων φορέων στο Metaverse, τόσο σε ενωσιακό επίπεδο - από το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (διεθνώς European Data Protection Board/EDPB, εφεξής «ΕΣΠΔ») -, όσο και σε εθνικό επίπεδο - από τις εποπτικές αρχές των κρατών-μελών-, ώστε να εξασφαλιστεί εκ των προτέρων η ενιαία και σύννομη ερμηνεία και εφαρμογή του ΓΚΠΔ στο Metaverse περιβάλλον.

Περαιτέρω, όμως, θα πρέπει να υιοθετηθούν και διαφανείς πολιτικές επεξεργασίας προσωπικών δεδομένων από τους εμπλεκόμενους φορείς, κάτι που όπως θα δούμε παρακάτω, αναμένεται να δημιουργήσει νέα ζητήματα προστασίας της ιδιωτικότητας στο Metaverse. Ταυτόχρονα, είναι καίριας σημασίας οι σχέσεις μεταξύ από κοινού υπευθύνων και υπευθύνων – εκτελούντων να ρυθμίζονται με σαφήνεια μέσω ειδικών συμφωνιών, όπως άλλωστε ορίζει ο ΓΚΠΔ στα άρθρα 26 και 28 αντίστοιχα, για τη συμμόρφωση προς την αρχή της λογοδοσίας. Έχει πάντως υποστηριχθεί και η ρηξικέλευθη άποψη περί κατάργησης της οριοθέτησης μεταξύ υπευθύνων και εκτελούντων ως προς ορισμένες υποχρεώσεις τους στο Metaverse, ώστε όλοι οι ευθυνόμενοι να εργάζονται από κοινού για τη συμμόρφωση προς τις διατάξεις του ΓΚΠΔ *("Abolishing the delineation between data controllers and processors will avoid a convoluted metaverse privacy policy…In the absence of labels for processors and controllers in the metaverse, companies will have to work together to avoid similar fines.")* [335].

3.3. Ενημέρωση των υποκειμένων και νόμιμες βάσεις επεξεργασίας

[334] Koehler, P. (2022) 'The Metaverse and some of its emerging challenges for data protection law' *Taylor Wessing*, 10 Οκτωβρίου. Διαθέσιμο στο: https://www.taylorwessing.com/en/insights-and-events/insights/2022/10/the-metaverse-and-some-of-its-emerging-challenges-for-data-protection-law [Πρόσβαση 6 Μαΐου 2023].

[335] Ό.π., Martin, B. (2022), σ. 258-259.

Η απονομή της ιδιότητας του υπευθύνου επεξεργασίας υπό το καθεστώς του ΓΚΠΔ, συνεπάγεται γι' αυτόν σωρεία υποχρεώσεων και ευθυνών[336]. Αναπόφευκτα, το εικονικό περιβάλλον θα εντείνει τις ήδη υπάρχουσες δυσκολίες εφαρμογής του ΓΚΠΔ εντός του WEB 2.0, ταυτόχρονα όμως θα αναδείξει νέες προκλήσεις για τα ευθυνόμενα μέρη κατά την εκπλήρωση των συναφών υποχρεώσεών τους, με κίνδυνο εκτεταμένων παραβιάσεων της ιδιωτικότητας των χρηστών.

3.3.1. Η απαίτηση διαφάνειας της επεξεργασίας

Η τριπλή αρχή της νομιμότητας, αντικειμενικότητας και διαφάνειας που θεσπίζει το άρθρο 5 παρ. 1 στοιχ. α' ΓΚΠΔ[337], η αρχή του περιορισμού του σκοπού του άρθρου 5 παρ. 1 στοιχ. β' ΓΚΠΔ[338] και η αρχή της διαφάνειας των άρθρων 12-14 ΓΚΠΔ[339], επιτάσσουν την ενημέρωση των υποκειμένων από τον υπεύθυνο για τη διενεργούμενη επεξεργασία των προσωπικών τους δεδομένων, που είτε συλλέγονται ευθέως από τα ίδια τα υποκείμενα (άρθρο 13 ΓΚΠΔ)[340] είτε αντλούνται από άλλη πηγή (άρθρο 14 ΓΚΠΔ)[341].

Η ενημέρωση αυτή πρέπει να παρέχεται με συνοπτικό, διαφανή, κατανοητό και εύκολα προσβάσιμο τρόπο, σε σαφή και απλή διατύπωση, γραπτώς ή με άλλα μέσα (μεταξύ άλλων, ηλεκτρονικώς) ή, υπό όρους, προφορικώς[342]. Περιλαμβάνει, ανάλογα με την περίπτωση, πλήθος πληροφοριών, όπως την ταυτότητα και τα στοιχεία επικοινωνίας του υπευθύνου, τους σκοπούς και τη νόμιμη βάση της επεξεργασίας, τις κατηγορίες των δεδομένων που τυγχάνουν επεξεργασίας, τυχόν αποδέκτες ή κατηγορίες αποδεκτών των δεδομένων, το χρονικό διάστημα αποθήκευσης αυτών, τα δικαιώματα του υποκειμένου, την ύπαρξη τυχόν αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένης της

---

[336] Συγκεκριμένες υποχρεώσεις και ευθύνες, αλλά πιο περιορισμένες, έχει και ο εκτελών την επεξεργασία, δυνάμει του ΓΚΠΔ.

[337] Τα δεδομένα «*υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων*».

[338] Τα δεδομένα «*συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς*».

[339] Η εν λόγω αρχή επιτάσσει και τη διαφάνεια των ανακοινώσεων που πραγματοποιούνται δυνάμει των άρθρων 15 έως 22 ΓΚΠΔ, δηλαδή στο πλαίσιο της άσκησης των δικαιωμάτων των υποκειμένων.

[340] Η ενημέρωση πρέπει να λαμβάνει χώρα κατά τη λήψη των δεδομένων (άρθρο 13 παρ. 1 ΓΚΠΔ).

[341] Πχ. από τρίτους υπεύθυνους επεξεργασίας, μεσίτες δεδομένων, δημόσια διαθέσιμες πηγές ή άλλα υποκείμενα δεδομένων. Σε αυτήν την περίπτωση, η ενημέρωση πρέπει να λαμβάνει χώρα σε εύλογο χρονικό διάστημα από τη συλλογή των δεδομένων, το αργότερο εντός μηνός (άρθρο 14 παρ. 3 στ. α' ΓΚΠΔ).

[342] Επίσης, μπορεί να παρέχεται συνδυαστικά με τυποποιημένα εικονίδια (άρθρο 12 παρ. 7 ΓΚΠΔ).

κατάρτισης προφίλ κ.ο.κ.[343] Ο ΓΚΠΔ δεν ορίζει τον τρόπο ή τον μορφότυπο με τον οποίο οι πληροφορίες αυτές θα γνωστοποιηθούν στο υποκείμενο, ωστόσο καθιστά σαφές ότι το τελευταίο δεν πρέπει να αναγκάζεται να τις αναζητά, αντίθετα ο υπεύθυνος οφείλει να τις παρέχει απευθείας ή να το κατευθύνει στο σημείο που αυτές παρατίθενται (πχ. μέσω αναδυόμενου παραθύρου, υπερσυνδέσμου κ.ά.)[344]. Οι ανωτέρω πληροφορίες πρέπει να είναι διαθέσιμες πριν, κατά τη διάρκεια και μετά τη λήξη της επεξεργασίας των δεδομένων, ώστε να διασφαλίζεται ότι το υποκείμενο μπορεί ανά πάσα στιγμή να κατανοήσει τη φύση και τα όριά της[345], ενώ κάθε μεταγενέστερη ουσιώδης αλλαγή τους πρέπει να του κοινοποιείται[346].

Στο σύγχρονο οικοσύστημα του WEB 2.0 (βλ. 2D ιστότοποι, εφαρμογές έξυπνων τηλεφώνων κ.ά.), η ενημέρωση των χρηστών έχει επικρατήσει να διενεργείται μέσω των γραπτών πολιτικών «απορρήτου» ή αλλιώς «προστασίας προσωπικών δεδομένων» (privacy policies). Από την άλλη, το 3D Metaverse θα τροφοδοτείται συνεχώς και σε πραγματικό χρόνο με τα προσωπικά δεδομένα των χρηστών, ώστε να τους προσφέρει μία εμβυθιστική (i.e., αδιάλειπτη και ρεαλιστική) και εξατομικευμένη εμπειρία. Αποτελεί, λοιπόν, μυστήριο με ποιο τρόπο θα ενημερώνονται επαρκώς τα υποκείμενα στο ζωντανό και διαλειτουργικό περιβάλλον του. Υποστηρίζεται ότι η σχετική ενημέρωση θα μπορεί να παρέχεται με ενιαίο τρόπο για όλο το Metaverse ή χωριστά για κάθε συμμετέχουσα οντότητα[347]. Ωστόσο, καμία από τις δύο προσεγγίσεις δεν φαίνεται να ικανοποιεί τις αυξημένες απαιτήσεις διαφάνειας του ΓΚΠΔ[348].

Αφενός, η ενιαία εκπλήρωση της σχετικής υποχρέωσης από όλους τους υπεύθυνους επεξεργασίας στο Metaverse μαζί, θα αντιβαίνει στην απαίτηση για συνοπτική, διαφανή και κατανοητή ενημέρωση, αφού η σχετική πολιτική απορρήτου θα είναι υπερβολικά

[343] Αν τα δεδομένα που συλλέγονται αρχικά πρόκειται να υποβληθούν σε περαιτέρω επεξεργασία (πχ. κατάρτιση προφίλ) για άλλο σκοπό (πχ. εμπορική προώθηση), τότε και ο σκοπός αυτός, αλλά και οι κατηγορίες δεδομένων που θα προκύψουν από την περαιτέρω αυτή επεξεργασία πρέπει να κοινοποιηθούν στο υποκείμενο, είτε κατά την αρχική συλλογή ή πριν την επακόλουθη επεξεργασία.

[344] Βλ. Ομάδα προστασίας δεδομένων του άρθρου 29, Κατευθυντήριες γραμμές σχετικά με τη διαφάνεια βάσει του κανονισμού 2016/679, της 11ης Απριλίου 2018. Διαθέσιμο στο https://www.dpa.gr/sites/default/files/2020-05/wp260rev01_el.pdf, σ. 9 και 23.

[345] European Union Agency for Network and Information Security (ENISA) (2017) *Privacy and data protection in mobile applications: A study on the app development ecosystem and the technical implementation of GDPR*. Κρήτη: ENISA. Διαθέσιμο στο: https://pure.uva.nl/ws/files/42887337/22302384.pdf, σ. 48.

[346] Βλ. ό.π., Κατευθυντήριες γραμμές σχετικά με τη διαφάνεια βάσει του κανονισμού 2016/679, σ. 21.

[347] Ό.π., Koehler, P. (2022).

[348] Ό.π.

μακροσκελής, δυσνόητη και τελικά αδιαφανής, λόγω της πληθώρας των στοχευόντων φορέων που θα δραστηριοποιούνται σε αυτό. Αφετέρου, ακόμη κι η διακριτή ενημέρωση από κάθε υπεύθυνο επεξεργασίας στο Metaverse χωριστά, θα είναι δύσκολο να είναι συνοπτική, διαφανής και κατανοητή, λόγω του εύρους, της έντασης και της τεχνικής πολυπλοκότητας (μέσω αλγορίθμων Τεχνητής Νοημοσύνης) της επεξεργασίας των προσωπικών δεδομένων που θα διενεργείται στις οικείες πλατφόρμες. Εκτός αυτού, σε αυτό το σενάριο η περιήγηση του χρήστη θα διακόπτεται επανειλημμένως[349], ιδίως αν η σχετική ενημέρωση λάβει τη μορφή αναδυόμενων μπροστά στα άβαταρ παραθύρων κάθε φορά που θα αλλάζουν εμπειρία[350], καταργώντας την έννοια της απόλυτης εμβύθισης και αυτή καθ' εαυτή τη λειτουργικότητα του εικονικού περιβάλλοντος.

Σε κάθε περίπτωση, ο κίνδυνος που ελλοχεύει πίσω από τέτοιου είδους γραπτές (text-based) και στατικές ενημερώσεις για την προστασία των προσωπικών δεδομένων, είναι οι χρήστες να τις προσπερνούν χωρίς να διαβάζουν τις ίδιες ή τις τροποποιήσεις τους ή χωρίς να κατανοούν ουσιαστικά το περιεχόμενό τους[351], λόγω της εξειδικευμένης γλώσσας που χρησιμοποιούν ή της τεχνικής πολυπλοκότητας που παρουσιάζουν. Αυτό συμβαίνει ήδη στο περιβάλλον του WEB 2.0. (βλ. την πρακτική "clickwrap" που επιτρέπει την αποδοχή των όρων ενός κειμένου, όπως της πολιτικής απορρήτου, με ένα κλικ, χωρίς την ανάγκη ανάγνωσής τους)[352]. Είναι δε απόλυτα βέβαιο ότι θα ισχύσει και στο Metaverse, όπου ο χρήστης θα ενδιαφέρεται για τη γρήγορη σύνδεση και την απρόσκοπτη εμβύθισή του στην εικονική κοινότητα, αδιαφορώντας για τις συνέπειες της μη ενημερωμένης παραχώρησης των προσωπικών του δεδομένων σε τρίτους φορείς. Εξάλλου, δεν είναι απίθανο οι υπεύθυνοι επεξεργασίας να υιοθετήσουν και ευθέως αδιαφανείς πρακτικές, όπως είναι η δευτερογενής επεξεργασία των προσωπικών δεδομένων των χρηστών για μη καθορισμένους σκοπούς, χωρίς την έγκαιρη ενημέρωσή τους.

3.3.2. Συναίνεση και άλλες νόμιμες βάσεις επεξεργασίας

[349] Todd, E. et al. (2022) 'Data protection and privacy' in 'The Reed Smith Guide to the Metaverse - 2nd Edition'. Διαθέσιμο στο: https://www.reedsmith.com/en/perspectives/metaverse/2022/08/data-protection-and-privacy.

[350] Ό.π., Κοντογεώργου, Π., Συρμακέζη, Ζ., Ζούλοβιτς, Μ. (2022), σ. 54.

[351] Καλπία, Ε. (2022) *Προστασία της ιδιωτικότητας των χρηστών των μέσων κοινωνικής δικτύωσης σε οικοσυστήματα έξυπνων κινητών*. Πειραιάς: Πανεπιστήμιο Πειραιώς, σ. 45.

[352] Ό.π., σ. 45.

Τα ίδια προβλήματα θα κληθούν να αντιμετωπίσουν οι υπεύθυνοι επεξεργασίας στην προσπάθεια να λάβουν την έγκυρη συναίνεση των χρηστών για την επεξεργασία των απλών και κυρίως των ευαίσθητων προσωπικών δεδομένων αυτών στο Metaverse (άρθρα 6 παρ. 1 στοιχ. α' και 9 παρ. 2 στοιχ. α' ΓΚΠΔ, αντίστοιχα).

Εν προκειμένω, ο ΓΚΠΔ ορίζει ρητά στο άρθρο 4 παρ. 11 τις προϋποθέσεις της έγκυρης συγκατάθεσης[353], την οποία χαρακτηρίζει ως «*κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, εν πλήρει επιγνώσει και αδιαμφισβήτητη*[354]*, με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν*». Η συγκατάθεση, λοιπόν, του χρήστη πρέπει να είναι (α) *ελεύθερη*, δηλαδή να εκφράζει την αληθινή βούλησή του, πράγμα το οποίο δεν συμβαίνει όταν εξαναγκάζεται[355], εκφοβίζεται ή παραπλανάται ή όταν δεν υπάρχει δυνατότητα ανάκλησης της παρεχόμενης συναίνεσης με τον ίδιο εύκολο τρόπο με τον οποίο δόθηκε και χωρίς δυσμενείς γι' αυτόν συνέπειες[356], (β) *συγκεκριμένη*, δηλαδή να παρέχεται διακριτά για κάθε επιδιωκόμενο σκοπό[357], (γ) *εν πλήρει επιγνώσει*, δηλαδή να παρέχεται ενημέρωση[358] τουλάχιστον για την ταυτότητα του υπευθύνου, τους σκοπούς κάθε επιμέρους πράξης επεξεργασίας, το είδος των δεδομένων που θα συλλεχθούν και θα χρησιμοποιηθούν, το δικαίωμα ανάκλησης της συγκατάθεσης, πληροφορίες σχετικά με τη χρήση των δεδομένων, ιδίως για την αυτοματοποιημένη λήψη

---

353 Βλ. και αιτιολογική σκέψη 32, 42 και 43 ΓΚΠΔ.

354 Διορθωτικό στον Κανονισμό (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων).

355 Πχ. όταν υπάρχει σαφής ανισότητα μεταξύ των μερών ή όταν η παροχή της συναίνεσης τίθεται ως προϋπόθεση για την εκτέλεση μιας σύμβασης, ενώ η εν λόγω επεξεργασία δεν είναι αναγκαία (βλ. αιτιολογική σκέψη 43 και άρθρο 7 παρ. 4 ΓΚΠΔ).

356 Βλ. άρθρο 7 παρ. 3 ΓΚΠΔ.

357 Βλ. αιτιολογική σκέψη 32 εδ. ε' ΓΚΠΔ. Η σταδιακή διεύρυνση ή σύγχυση των σκοπών για τους οποίους τα δεδομένα υποβάλλονται σε επεξεργασία, μετά τη συναίνεση του υποκειμένου στην αρχική συλλογή τους καλείται «υφέρπουσα διεύρυνση λειτουργιών» και αντιβαίνει προς τις διατάξεις του ΓΚΠΔ (βλ. Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, Κατευθυντήριες γραμμές 5/2020 σχετικά με τη συγκατάθεση βάσει του κανονισμού 2016/679, Έκδοση 1.1, της4ης Μαΐου 2020. Διαθέσιμο στο: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_el.pdf, σ. 16.)

358 Σύμφωνα με τις Κατευθυντήριες γραμμές 5/2020, «*έγκυρες πληροφορίες μπορούν να παρέχονται με διάφορους τρόπους, όπως με γραπτές ή προφορικές δηλώσεις ή με ακουστικά ή οπτικά μηνύματα*» (βλ. ό.π., σ. 19).

αποφάσεων, και εάν η συγκατάθεση περιλαμβάνει και διαβίβαση, αναφορά των κινδύνων από τη διαβίβαση αυτή[359] και (δ) *αδιαμφισβήτητη*, δηλαδή να παρέχεται με σαφή θετική ενέργεια του υποκειμένου, για παράδειγμα με γραπτή δήλωσή του[360], μεταξύ άλλων με ηλεκτρονικά μέσα[361], ή προφορική δήλωσή του. Επιπλέον, αν πρόκειται να δοθεί κατόπιν αιτήματος με ηλεκτρονικά μέσα, το αίτημα αυτό θα πρέπει να χαρακτηρίζεται από σαφήνεια, μεστότητα και να μη διαταράσσει αδικαιολόγητα τη χρήση της υπηρεσίας[362].

Εκ των ανωτέρω προκύπτει ότι η παροχή έγκυρης συναίνεσης για την επεξεργασία των απλών προσωπικών δεδομένων των χρηστών υπό το άρθρο 6 παρ. 1 στοιχ. α' ΓΚΠΔ δύσκολα θα μπορούσε να επιτευχθεί στο Metaverse. Το ίδιο ισχύει και για την επεξεργασία των ευαίσθητων προσωπικών δεδομένων τους, για τη νομιμότητα της οποίας θα πρέπει να παρέχουν ελεύθερη, συγκεκριμένη, ενημερωμένη και αδιαμφισβήτητη συναίνεση για κάθε ειδικότερο σκοπό επεξεργασίας υπό το άρθρο 9 παρ. 2 στοιχ. α' ΓΚΠΔ. Κρίνοντας από το σύγχρονο στατικό πρότυπο λήψης συναίνεσης που έχουν υιοθετήσει οι πάροχοι στο WEB 2.0 (βλ. clickwrap και γραπτές πολιτικές απορρήτου), την αντιμετώπιση των χρηστών που σπάνια διαβάζουν - πόσο μάλλον αντιλαμβάνονται - τα σχετικά κείμενα[363] (βλ. consent fatigue), αλλά και τις καταχρηστικές πρακτικές των παρόχων (βλ. dark patterns[364], cookie walls κ.ά.), είναι σίγουρο ότι στο Metaverse, τίποτα δεν θα αλλάξει. Ακόμα χειρότερα, οι σχετικές πολιτικές απορρήτου θα είναι πολύ πιο μακροσκελείς, δυσνόητες και αδιαφανείς, ενώ η ουσιαστική εμβύθιση των χρηστών, εξαρτώμενη από την απρόσκοπτη μετακίνησή τους εντός του 3D εικονικού σύμπαντος, θα καθιστά την παροχή έγκυρης συναίνεσης πρακτικά αδύνατη. Ιδιαίτερα εάν αναλογιστεί κανείς πως μόνο 20 λεπτά εμπειρίας στην εικονική πραγματικότητα ισοδυναμούν με δύο εκατομμύρια (!) μηχανικές καταγραφές της

[359] Βλ. αιτιολογική σκέψη 42 ΓΚΠΔ σε συνδυασμό με Κατευθυντήριες Γραμμές 5/2020, σ. 18.

[360] Σε περίπτωση γραπτής δήλωσης που αφορά και σε άλλα θέματα, το αίτημα για τη συγκατάθεση θα πρέπει να υποβάλλεται διακριτά από τα υπόλοιπα, σε κατανοητή και εύκολα προσβάσιμη μορφή, χωρίς καταχρηστικούς όρους (βλ. άρθρο 7 παρ. 2 ΓΚΠΔ).

[361] Αυτό θα μπορούσε να περιλαμβάνει, ενδεικτικά, τη συμπλήρωση ενός τετραγωνιδίου κατά την επίσκεψη σε διαδικτυακή ιστοσελίδα, την αποστολή e-mail, τη συμπλήρωση ηλεκτρονικής φόρμας, την ηλεκτρονική υπογραφή κ.ο.κ. Αντίθετα, η σιωπή, η αδράνεια, η χρήση προσυμπληρωμένων τετραγωνιδίων ή η συμπερίληψη της συγκατάθεσης σε προδιατυπωμένους όρους ΓΟΣ δεν ικανοποιούν τις προϋποθέσεις του νόμου (βλ. αιτιολογική σκέψη 32 ΓΚΠΔ).

[362] Βλ. αιτιολογική σκέψη 32 ΓΚΠΔ, τελευταίο εδάφιο.

[363] Ό.π., Anidjar, L.Y., Packin, N.G. and Panezi, A. (2023), σ. 45.

[364] Ό.π.

γλώσσας του σώματός τους[365], αντιλαμβάνεται πως είναι ανθρωπίνως αδύνατο για τα υποκείμενα να παρέχουν ενεργό συναίνεση για την ταυτόχρονη και σε πραγματικό χρόνο επεξεργασία των βιομετρικών και βιομετρικού τύπου δεδομένων τους από το πλήθος υπευθύνων που θα δραστηριοποιούνται στο Metaverse και για το πλήθος σκοπών που θα υπηρετούν. Στο ίδιο μήκος κύματος, αμφισβητείται αν η συναίνεση των χρηστών θα πληροί τα απαιτούμενα κριτήρια νομιμότητας για την επεξεργασία άλλων ευαίσθητων πληροφοριών τους, όπως τα πολιτικά φρονήματα ή τα δεδομένα υγείας τους, που θα διενεργείται συνεχώς στο πλαίσιο της προώθησης εμπορικών, πολιτικών ή άλλων συμφερόντων των υπευθύνων. Πέραν τούτων, είναι πολύ πιθανό οι τελευταίοι να ζητούν τη συναίνεση των χρηστών με ενιαίο τρόπο για περισσότερους σκοπούς, να επεξεργάζονται προσωπικά δεδομένα τους για σκοπούς ασύμβατους με αυτούς για τους οποίους οι χρήστες αρχικά συναίνεσαν ή προσωπικά δεδομένα τα οποία αυθαίρετα συνάγουν από αυτά για τα οποία δόθηκε αρχικά η συναίνεση. Η συγκατάθεση, άλλωστε, δεν θα μπορεί να θεωρηθεί ελεύθερη, εφόσον η επεξεργασία θα είναι απαραίτητη για τη ρεαλιστική απόδοση των κινήσεων τους στον εικονικό κόσμο, με αποτέλεσμα να μη τους παρέχεται εναλλακτική λύση, ή σε περιπτώσεις που θα τίθεται ως προϋπόθεση για την εκτέλεση της σύμβασης παροχής υπηρεσιών Metaverse, ενώ επί της ουσίας η οικεία επεξεργασία δεν θα είναι απολύτως απαραίτητη[366].

Τελικά, ποιες νόμιμες βάσεις του ΓΚΠΔ κρίνονται κατάλληλες και αναμένεται να χρησιμοποιηθούν για την επεξεργασία των προσωπικών δεδομένων των χρηστών στο Metaverse, *υπό το ισχύον νομοθετικό καθεστώς*;

Απλά προσωπικά δεδομένα: Η νόμιμη βάση η οποία αναμένεται να λειτουργήσει ως «ομπρέλα» για να δικαιολογήσει τις περισσότερες πράξεις επεξεργασίας αυτού του είδους προσωπικών δεδομένων, είναι το άρθρο 6 παρ. 1 στοιχ. β' ΓΚΠΔ. Θα μπορεί να εφαρμοστεί, εφόσον η οικεία επεξεργασία κριθεί απαραίτητη για την εκτέλεση της σύμβασης παροχής υπηρεσιών Metaverse ή για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου πριν από τη σύναψή της[367]. Η εν λόγω διάταξη θα μπορούσε, λοιπόν, να θεωρηθεί νόμιμη βάση για την επεξεργασία της IP διεύθυνσης, των στοιχείων διεύθυνσης, επικοινωνίας και πληρωμής

[365] Ό.π., Κοντογεώργου, Π., Συρμακέζη, Ζ., Ζούλοβιτς, Μ. (2022), σ. 53.

[366] Βλ. Olivi, G., Anselmi, N. and Miele, C.O. (2020) 'Virtual Reality: Top Data Protection Issues to Consider' *The Journal of Robotics, Artificial Intelligence & Law*, 3(2), σ. 141-145. Διαθέσιμο στο: https://search.informit.org/doi/10.3316/agispt.20230202082765, σ. 143, για VR.

[367] Ό.π., Bolognini, L. and Carpenelli, M. E. (2022), σ. 10.

των χρηστών[368] και των δεδομένων θέσης τους, αλλά και για το σύνολο των βιομετρικού τύπου δεδομένων που θα είναι απαραίτητα για τη ρεαλιστική απόδοση της δραστηριότητάς τους στο εικονικό περιβάλλον και θα χρησιμοποιούνται με σκοπό την ταυτοποίηση του ψυχογραφικού προφίλ τους, και που σήμερα δεν συγκαταλέγονται ευθέως στα βιομετρικά δεδομένα (πχ. κινήσεις ματιών, κατεύθυνση βλέμματος, εκφράσεις προσώπου, βαθμός εφίδρωσης κ.ο.κ.). Το ΕΣΠΔ έχει κρίνει, πάντως, ότι δεν είναι κατ' αρχήν αναγκαία για την εκτέλεση της σύμβασης η επεξεργασία προσωπικών δεδομένων του αντισυμβαλλόμενου ούτε για τη βελτίωση της παρεχόμενης επιγραμμικής υπηρεσίας[369] ούτε για σκοπούς συμπεριφορικής διαφήμισης και κατάρτισης ατομικού προφίλ[370], ενώ αντίθετα, θεωρεί ότι η εξατομίκευση του προβαλλόμενου περιεχομένου ενδέχεται να αποτελέσει εγγενές και προσδοκώμενο στοιχείο ορισμένων επιγραμμικών υπηρεσιών, με κριτήριο τη φύση της παρεχόμενης υπηρεσίας και τις εύλογες προσδοκίες του υποκειμένου[371]. Είναι αρκετά πιθανόν, λοιπόν, η εξατομίκευση να θεωρηθεί σύμφυτη με το ρεαλιστικό περιβάλλον που το Metaverse επιδιώκει να διαμορφώσει και συνεπώς, ευλόγως αναμενόμενη από τους χρήστες του. Ωστόσο, στον εικονικό κόσμο, τόσο η προσωποποίηση του προβαλλόμενου περιεχομένου όσο και η συμπεριφορική διαφήμιση θα μετέρχονται τα ίδια ισχυρά μέσα χειραγώγησης των υποκειμένων, υπό την έννοια ότι θα βασίζονται αμφότερες στη σύγχρονη παρακολούθηση των εν ευρεία έννοια βιομετρικών δεδομένων τους και στη σταδιακή κατάρτιση του ατομικού προφίλ τους. Κατά συνέπεια, υπάρχει ο κίνδυνος να νομιμοποιηθεί ως αναγκαία η επεξεργασία των βιομετρικού τύπου πληροφοριών του χρήστη και για σκοπούς απευθείας εμπορικής προώθησης, πληροφοριών σχετικών με τις ασυνείδητες φυσικές, βιολογικές και συμπεριφορές αντιδράσεις του σε εξωτερικά

[368] Πχ. η επεξεργασία των εν λόγω προσωπικών δεδομένων είναι απαραίτητη για την πραγματοποίηση συναλλαγών από τους χρήστες μέσω του Metaverse.

[369] Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, Κατευθυντήριες γραμμές 2/2019 για την επεξεργασία δεδομένων προσωπικού χαρακτήρα σύμφωνα με το άρθρο 6 παράγραφος 1 στοιχείο β) του ΓΚΠΔ στο πλαίσιο της παροχής επιγραμμικών υπηρεσιών σε υποκείμενα δεδομένων, Έκδοση 2.0, της 8ης Οκτωβρίου 2019. Διαθέσιμο στο: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_el.pdf, σ. 17.

[370] Ό.π., σ. 17 επ. Δηλαδή, το υποκείμενο συμβάλλεται για να του παρασχεθεί η σχετική υπηρεσία και όχι για να του προβληθούν διαφημίσεις βάσει της συμπεριφοράς του.

[371] Δυνάμει των όρων της σύμβασης και του πώς προωθείται η υπηρεσία στο υποκείμενο. Ό.π., σ. 18 επ.

ερεθίσματα και για τις οποίες δεν θα απαιτείται καν η συναίνεσή του για να τις συλλέξουν και αξιοποιήσουν οι οικείοι πάροχοι.

Συμπληρωματικά, οι υπεύθυνοι επεξεργασίας στο Metaverse θα μπορούσαν νομίμως να επικαλεσθούν το άρθρο 6 παρ. 1 στοιχ. στ' ΓΚΠΔ, εφόσον η οικεία επεξεργασία κριθεί απαραίτητη για την επιδίωξη των εννόμων συμφερόντων τους, υπό την προϋπόθεση ότι αυτά υπερισχύουν των συμφερόντων και των θεμελιωδών δικαιωμάτων και ελευθεριών των φυσικών προσώπων που υπαγορεύουν την προστασία των προσωπικών δεδομένων τους. Σύμφωνα με την αιτιολογική σκέψη 47 ΓΚΠΔ, κατά τη στάθμιση αυτή, θα πρέπει να λαμβάνονται υπόψη οι θεμιτές προσδοκίες των υποκειμένων, δυνάμει της σχέσης που τα συνδέει με τον υπεύθυνο, το αν δηλαδή μπορούν να αναμένουν εύλογα, κατά τη χρονική στιγμή και στο πλαίσιο της συλλογής των δεδομένων τους, περαιτέρω επεξεργασία αυτών από τον υπεύθυνο. Σύμφωνα με το τελευταίο εδάφιο της ως άνω αιτιολογικής σκέψης, η άμεση εμπορική προώθηση θα μπορούσε να θεωρηθεί ότι ανήκει στα έννομα συμφέροντα του υπευθύνου. Ο Yeji Kim αναφέρει χαρακτηριστικά ότι όσο περισσότερο τα υποκείμενα βιώνουν την Εικονική Πραγματικότητα ως μια υπηρεσία κοινωνικής δικτύωσης (Social Network Service/SNS), τόσο περισσότερο η επεξεργασία των προσωπικών δεδομένων τους για σκοπούς εμπορικής προώθησης θα εμπίπτει στις θεμιτές προσδοκίες τους[372]. Έτσι, για παράδειγμα, η επεξεργασία των δημογραφικών στοιχείων (πχ. φύλο, ηλικία, επάγγελμα κ.ά.), αλλά και των βιομετρικού τύπου δεδομένων των χρηστών του Metaverse για σκοπούς διαφήμισης, θα είναι δυνατόν να θεωρηθεί ότι εμπίπτει στα έννομα συμφέροντα των σχετικών παρόχων. Ωστόσο, μια συνολική θεώρηση του τι συνιστά «θεμιτή προσδοκία» θα μπορούσε να παραβλέψει τυχόν διαφορετικές εντυπώσεις ή προσδοκίες των υποκειμένων για τις λειτουργικές σκοπιμότητες του Metaverse[373], αν και η σταδιακή επικράτησή του ως ενός παράλληλου με τον πραγματικό εικονικού κόσμου ίσως να εξομοίωνε εν πολλοίς τις όποιες ασυμφωνίες.

Προσωπικά δεδομένα ειδικών κατηγοριών: Υπό το ισχύον καθεστώς του ΓΚΠΔ, ικανοποιητική νόμιμη βάση για την επεξεργασία των ευαίσθητων προσωπικών δεδομένων των χρηστών στο Metaverse παρίσταται μόνο το άρθρο 9 παρ. 2 στοιχ. ε', για τα δεδομένα εκείνα που ο ίδιος ο χρήστης *προδήλως* θα δημοσιοποιεί. Σύμφωνα με τις Κατευθυντήριες γραμμές 8/2020 σχετικά με τη στόχευση χρηστών μέσων κοινωνικής δικτύωσης, πρέπει να

[372] Ό.π., Kim, Y. (2022), σ. 250.

[373] Βλ. Kim, Y. (2022), σ. 250, για VR.

γίνεται κατά περίπτωση εκτίμηση του αν το υποκείμενο έχει δημοσιοποιήσει προδήλως ευαίσθητα προσωπικά δεδομένα του, ενώ το επίπεδο απόδειξης πρέπει να είναι υψηλό[374]. Τα προτεινόμενα κριτήρια για την εν λόγω εκτίμηση είναι η αλλαγή από το χρήστη των εξ ορισμού ιδιωτικών ρυθμίσεων του λογαριασμού σε δημόσιες, η φύση της πλατφόρμας ως χώρου σμίλευσης ευρύτερων διαπροσωπικών σχέσεων, η ελεύθερη προσβασιμότητα της οικείας σελίδας, η δημοσίευση των δεδομένων από το ίδιο το υποκείμενο και όχι από τρίτον ή μέσω συναγωγής[375] κ.ά. Δυνάμει των ανωτέρω, ένας χρήστης του Metaverse θα μπορούσε να θεωρηθεί ότι δημοσιοποιεί προδήλως ευαίσθητα προσωπικά δεδομένα του, αν επιλέγει να διαμορφώσει ένα άβαταρ με τα δικά του ατομικά χαρακτηριστικά σε ένα ανοιχτό Metaverse[376] ή ενώ έχει επιλέξει ενεργά δημόσιες ρυθμίσεις για τον προσωπικό λογαριασμό του. Μολαταύτα, αυτό δεν θα μπορούσε να ισχύει για τα βιομετρικά δεδομένα του χρήστη, η επεξεργασία των οποίων θα είναι εκ των πραγμάτων αναγκαία για την αδιαμφισβήτητη ταυτοποίησή του (πχ. για σκοπούς ασφαλείας) ή την αληθοφανή εμβύθισή του στην πλατφόρμα[377], αλλά ούτε και για τα ευαίσθητα εκείνα δεδομένα που οι πάροχοι θα μπορούν να συνάγουν από το συνδυασμό των παρεχόμενων από το χρήστη ή των παρατηρήσιμων από αυτούς δεδομένων. Κατ' αποτέλεσμα, δεν θα μπορεί να θεωρηθεί, για παράδειγμα, ότι ο χρήστης προδήλως δημοσιοποιεί στους οικείους παρόχους την ίριδα του ματιού του, το κινησιολογικό του αποτύπωμα (*"kinematic fingerprint"*)[378] ή δεδομένα υγείας του που συνάγονται μέσω eye-tracking τεχνολογιών.

Είναι δεδομένο, λοιπόν, ότι στο Metaverse, η διασφάλιση της διαφάνειας και της νομιμότητας της επεξεργασίας θα αποδειχθεί ιδιαίτερα δυσχερής, αν όχι ανεδαφική υπό το ισχύον νομοθετικό καθεστώς και τις βάσει αυτού υιοθετούμενες πρακτικές. Τα κυριότερα προβλήματα εντοπίζονται στη δυσχέρεια διαφανούς ενημέρωσης και εξασφάλισης της έγκυρης (ελεύθερης, ενημερωμένης, συγκεκριμένης και αδιαμφισβήτητης) συναίνεσης των χρηστών για την επεξεργασία των προσωπικών τους δεδομένων σε ένα άκρως διαδραστικό

---

[374] Ό.π., Κατευθυντήριες 8/2020, σ. 43 επ.

[375] Ό.π.

[376] Ό.π., Lumley, C. (2022).

[377] Ό.π., Καρδαμάκη, Α. (2022).

[378] Madary, M. and Metzinger, T. K. (2016) 'Real Virtuality: A Code of Ethical Conduct. Recommendations for Good Scientific Practice and the Consumers of VR-Technology', *Frontiers in Robotics & AI*, 3 (No 3). Διαθέσιμο στο: https://www.frontiersin.org/articles/10.3389/frobt.2016.00003/full. Ο τρόπος που κινείται ένας άνθρωπος μπορεί να τον συνδέσει μοναδικά με την ταυτότητά του, εν είδει *«κινησιολογικού αποτυπώματος»*.

οικοσύστημα και στην ανάδειξη της μαζικής επεξεργασίας βιομετρικών και βιομετρικού τύπου δεδομένων σε αναγκαία προϋπόθεση λειτουργικότητας του συστήματος. Όλα αυτά, σε συνδυασμό με το ότι οι ως άνω βιομετρικού τύπου πληροφορίες δεν προστατεύονται σήμερα ρητώς από τον ΓΚΠΔ ως ευαίσθητα δεδομένα, ζωγραφίζουν με μελανά χρώματα το μέλλον της ιδιωτικότητας των χρηστών στο Metaverse. Συγκεκριμένα, η επεξεργασία των πληροφοριών αυτών θα καλύπτεται υπό το πέπλο μίας άκυρης, τυπικά παρεχόμενης συναίνεσής τους (άρθρο 6 παρ. 1 στοιχ. α' ΓΚΠΔ) ή θα νομιμοποιείται ως απολύτως αναγκαία για τη λειτουργία του συστήματος[379] (άρθρο 6 παρ. 1 στοιχ. β' ΓΚΠΔ) ή ως ανήκουσα στη σφαίρα των εννόμων συμφερόντων των παρόχων (άρθρο 6 παρ. 1 στοιχ. στ' ΓΚΠΔ). Την ίδια άκυρη συναίνεση θα δίνουν οι χρήστες και για την επεξεργασία των εν στενή εννοία βιομετρικών και των λοιπών ευαίσθητων προσωπικών τους δεδομένων που δεν δημοσιοποιούν *προδήλως* στο Metaverse. Σε κάθε περίπτωση, αν τίποτα δεν αλλάξει, θα συναινούν αναγκαστικά στην επεξεργασία, χωρίς να γνωρίζουν ποια δεδομένα θα υπόκεινται σε αυτήν, για ποιους σκοπούς, για πόσο και από ποιους αυτή θα διενεργείται, ή απλώς θα παρακολουθούνται παράνομα, στο παρασκήνιο ("*data will be gathered in the background while they go about their virtual lives")*[380].

Για τους λόγους αυτούς, όπως προτάθηκε και σε προηγούμενη ενότητα (υπό 3.1.), ο ΓΚΠΔ πρέπει να τροποποιηθεί, ούτως ώστε να συμπεριληφθούν στις ειδικές κατηγορίες προσωπικών δεδομένων και δη στα βιομετρικά, οι βιομετρικού τύπου πληροφορίες του χρήστη που θα καταγράφονται συνεχώς από τους παρόχους πρόσβασης και εμβύθισης στο Metaverse και θα αξιοποιούνται επιπρόσθετα *με σκοπό* την ταυτοποίηση των προτιμήσεων και γενικότερα, της προσωπικότητάς του[381]. Επιπλέον, προτείνεται να συμπεριληφθεί στις

---

[379] Ό.π., Mangada Real de Asúa, E. et al. (2022), σ. 16.

[380] Ό.π., Murphy, S. et al. (2021).

[381] Σύμφωνα με τη γνώμη των Bolognini και Carpenelli, η επεξεργασία των «*ανθρώπινων χαρακτηριστικών*» του χρήστη, όσων σχετίζονται δηλαδή «*με δεδομένα παρακολούθησης των χεριών, του σώματος, του προσώπου, του κεφαλιού ή των ματιών*» του, θα μπορούσε να υπαχθεί στο άρθρο 6 παρ. 1 στοιχ. β' ΓΚΠΔ και να θεωρηθεί αναγκαία (για τη λειτουργία του Metaverse) επεξεργασία απλών προσωπικών δεδομένων, εφόσον θα πραγματοποιείται μόνο προς το σκοπό ρεαλιστικής εμβύθισης του χρήστη στην εικονική πλατφόρμα (βλ. ό.π., Bolognini, L. and Carpenelli, M. E. (2022), σ. 5 επ.). Από την άλλη, σύμφωνα πάλι με την ίδια γνώμη, τα «*συναγόμενα δεδομένα*» που οποιοδήποτε τρίτο μέρος θα μπορεί να συνάγει από την ανάλυση των «*ανθρώπινων χαρακτηριστικών*» του, θα μπορούσαν να αποτελέσουν ευαίσθητα προσωπικά δεδομένα υπό τους όρους του άρθρου 9 ΓΚΠΔ (πχ. δεδομένα υγείας) (βλ. ό.π., σ. 8). Κατά τη γνώμη της γράφουσας, η άποψη αυτή παραγνωρίζει το γεγονός ότι τα τεχνολογικά εργαλεία που θα χρησιμοποιούν οι οικείοι πάροχοι για τη συλλογή των δεδομένων θα ενέχουν ειδικές τεχνικές επεξεργασίας των εν λόγω

νόμιμες βάσεις επεξεργασίας των δεδομένων ειδικών κατηγοριών αντίστοιχη διάταξη με αυτήν του στοιχ. β' της παρ. 1 του άρθρου 6 ΓΚΠΔ, μόνο για την επεξεργασία βιομετρικών δεδομένων σε εικονικά περιβάλλοντα. Με αυτόν τον τρόπο, τα *απολύτως αναγκαία* για τη ρεαλιστική εμβύθιση των χρηστών βιομετρικά δεδομένα τους (συμπεριλαμβανομένων πια και των βιομετρικού τύπου πληροφοριών τους), θα τυγχάνουν νόμιμης επεξεργασίας υπό τον ΓΚΠΔ. Στο πλαίσιο αυτό, σύμφωνα με όσα αναλύθηκαν ανωτέρω (ενότητα υπό 3.1.), είναι άκρως σημαντικό να δοθεί ρυθμιστική καθοδήγηση από τις αρμόδιες αρχές σχετικά με το *ποια ακριβώς* βιομετρικά δεδομένα παρίσταται απολύτως αναγκαίο να υποβάλλονται σε επεξεργασία για τη ρεαλιστική εμβύθιση των χρηστών και την ουσιαστική λειτουργία του Metaverse. Περαιτέρω, θα πρέπει να καθοριστεί με ακρίβεια *ποιοι άλλοι σκοποί* συγκαταλέγονται στην ουσιαστική αυτή λειτουργία (πχ. η εξατομίκευση του περιεχομένου και η συμπεριφορική διαφήμιση μπορούν να θεωρηθούν σκοποί αναγκαίοι για την εκτέλεση της σύμβασης παροχής υπηρεσιών Metaverse;). Ως προς τις υπόλοιπες μη αναγκαίες πράξεις επεξεργασίας και μη αναγκαίους σκοπούς για την ουσιαστική λειτουργία του Metaverse, οι χρήστες πρέπει να έχουν *ελεύθερη* επιλογή να δημοσιοποιήσουν ή όχι τα προσωπικά δεδομένα τους.

Σε περιβάλλοντα Εικονικής Πραγματικότητας, έχει υποστηριχθεί ότι η αυτονομία των χρηστών θα μπορούσε ενδεικτικά να προφυλαχθεί με: (α) τη ρύθμιση της υποχρέωσης των παρόχων των συσκευών VR να υιοθετούν παραμετροποιήσιμες ρυθμίσεις απορρήτου (customizable privacy settings), δυνάμει των οποίων ο χρήστης θα μπορεί να επιλέγει αυτόνομα σε ποιο βαθμό τα βιομετρικά δεδομένα του θα υπόκεινται σε επεξεργασία για την εξατομίκευση του προβαλλόμενου περιεχομένου[382] και (β) την υιοθέτηση δημιουργικών τρόπων ενημέρωσης και λήψης της συναίνεσης των χρηστών[383], πχ. μέσω μικρού μήκους βίντεο που θα προβάλλονται σε αυτούς πριν την παροχή της συναίνεσης, και μέσω της

δεδομένων, που θα επιτρέπουν και θα στοχεύουν στην εξακρίβωση είτε της ταυτότητας του υποκειμένου ή του ψυχογραφικού προφίλ του (και ακολούθως, την εξατομίκευση του περιεχομένου, τη συμπεριφορική διαφήμιση κ.ο.κ.). Κατ' επέκταση, η επεξεργασία τους θα αναβαθμίζεται αυτομάτως σε επεξεργασία προσωπικών δεδομένων ειδικών κατηγοριών, τα εν λόγω δεδομένα θα πρέπει να χαρακτηρίζονται βιομετρικά δεδομένα και άρα, να υπόκεινται στο προστατευτικό πεδίο του άρθρου 9 ΓΚΠΔ.

[382] Ό.π., Kim, Y. (2022), σ. 253.

[383] Ό.π., European Data Protection Supervisor (2019), σ. 8.

επακόλουθης συμμετοχής τους σε διαδραστικές ασκήσεις για να αντιληφθούν εκ των προτέρων τη σπουδαιότητα και τις ενδεχόμενες συνέπειες των επιλογών τους[384].

Το υπό (β) θα μπορούσαν να εφαρμόζουν και οι πάροχοι πρόσβασης και εμβύθισης στο Metaverse και κάθε από κοινού με αυτούς υπεύθυνος επεξεργασίας πριν την αρχική είσοδο των χρηστών σε αυτό, αλλά και κάθε υπεύθυνος επεξεργασίας που θα δραστηριοποιείται στον εικονικό χώρο πριν την πρώτη χρήση των υπηρεσιών του από τους χρήστες - τόσο για τη διαφανή ενημέρωση των υποκειμένων, όσο και για τη λήψη της έγκυρης συναίνεσης αυτών για την επεξεργασία των προσωπικών δεδομένων τους για μη αναγκαίους για τη λειτουργία του Metaverse σκοπούς. Η οπτικοποίηση των πολιτικών απορρήτου πρέπει, λοιπόν, να προβλεφθεί ρητώς στον ΓΚΠΔ ως απαραίτητη σε εικονικά περιβάλλοντα, ώστε να μην καταλείπεται περιθώριο στους παρόχους να εμμένουν σε στατικές μεθόδους ενημέρωσης και λήψης συναίνεσης. Για την αποτελεσματικότητα της οπτικοποίησης, προτείνεται οι οικείοι πάροχοι να υποχρεούνται να παρέχουν εγκαίρως αναλυτικές πληροφορίες στο αρμόδιο εποπτικό όργανο για τον τρόπο με τον οποίο θα απεικονίζουν οπτικά τους όρους των σχετικών πολιτικών τους[385], για να τους παρέχεται η απαραίτητη καθοδήγηση για τη βελτιστοποίηση αυτών. Από την άλλη, η δυνατότητα των χρηστών να ρυθμίζουν αυτόνομα το βαθμό εξατομίκευσης της 3D εμπειρίας μέσω παραμετροποιήσιμων ρυθμίσεων απορρήτου, είναι πολύ πιθανό να διακυβεύσει την ίδια τη φύση και το σκοπό του εικονικού κόσμου[386], αν και θα συνιστούσε βέλτιστη πρακτική για την προστασία της ιδιωτικότητας τους.

Σε γενικό πλαίσιο, το ζήτημα της διαφάνειας και της νομιμότητας της επεξεργασίας είναι κομβικής σημασίας για την επεξεργασία των προσωπικών δεδομένων των χρηστών στο Metaverse και γι' αυτό το λόγο θα πρέπει να δοθεί εγκαίρως η απαραίτητη ρυθμιστική καθοδήγηση από τις αρμόδιες αρχές, για να διαλευκανθούν όλες οι αμφιλεγόμενες πτυχές που θα απασχολήσουν τους συμμετέχοντες. Μεταξύ άλλων, θα πρέπει να αποσαφηνιστεί πώς θα μπορούσαν να ειδοποιούνται επαρκώς οι τρίτοι που βρίσκονται στον περιβάλλοντα χώρο του χρήστη και να λαμβάνεται εγκύρως η συναίνεσή τους για την όποια επεξεργασία των προσωπικών δεδομένων τους, τι θα μπορούσε να θεωρηθεί ως *πρόδηλη* δημοσιοποίηση των ευαίσθητων δεδομένων των χρηστών στο Metaverse, ποιοι σκοποί θα μπορούσαν να

---

[384] Ό.π., Kim, Y. (2022), σ. 255.

[385] Ό.π., Anidjar, L.Y., Packin, N.G. and Panezi, A. (2023), σ. 46.

[386] "*In a way, restricting customization would defeat the purpose of experiencing virtual reality"*(βλ. ό.π., Kim, Y. (2022), σ. 254, για VR.

θεωρηθούν συμβατοί με την αρχική συλλογή των δεδομένων για τη ρεαλιστική απεικόνιση τους στην εικονική πλατφόρμα κ.ο.κ. Συμπληρωματικά, θα πρέπει να ενθαρρύνεται η εκπόνηση κωδίκων δεοντολογίας και η θέσπιση μηχανισμών πιστοποίησης, που θα εφαρμόζονται από τους συμμετέχοντες στο Metaverse, για τη συμμόρφωσή τους προς τον ΓΚΠΔ.

3.4. Συμπεριφορική διαφήμιση και αλγοριθμική λήψη αποφάσεων

Στη δυστοπική εκδοχή του Metaverse, η μέθοδος της συμπεριφορικής διαφήμισης[387] [388]και η αλγοριθμική λήψη αποφάσεων θα γνωρίσουν αμφότερες μία τρομακτική δυναμική, οδηγώντας σε ακραία οικονομική και πολιτική χειραγώγηση (manipulation), απώλεια ατομικής αυτονομίας (loss of autonomy) και ενίσχυση των προκαταλήψεων (bias) και των διακρίσεων (discrimination) εις βάρος των χρηστών του.

---

[387] Η συμπεριφορική διαφήμιση είναι η προβολή διαφημιστικού περιεχομένου που βασίζεται στην εις βάθος χρόνου παρακολούθηση της συμπεριφοράς των χρηστών του Διαδικτύου, με σκοπό την δημιουργία εκτενών προφίλ χρηστών και την επακόλουθη προώθηση στοχοθετημένης διαφήμισης, βάσει των ενδιαφερόντων και των προτιμήσεών τους. Η κυριότερη τεχνολογία παρακολούθησης είναι προς το παρόν τα γνωστά σε όλους "cookies". Για τα cookies και τον τρόπο λειτουργίας τους, βλ. Ομάδα προστασίας δεδομένων του άρθρου 29, Γνώμη 2/2010 σχετικά με την επιγραμμική συμπεριφορική διαφήμιση, της 22ας Ιουνίου 2010. Διαθέσιμο στο: https://www.dpa.gr/sites/default/files/2019-10/WP171_EL.PDF, σ. 6 επ. Τον τελευταίο καιρό, πάντως, φημολογείται έντονα ότι τα third-party cookies βρίσκονται στη δύση της κυριαρχίας τους (Gozman, V. (2022) 'The Slow Death Of Third-Party Cookies', *Forbes*, 12 Σεπτεμβρίου. Διαθέσιμο στο: https://www.forbes.com/sites/theyec/2022/09/12/the-slow-death-of-third-party-cookies/?sh=2dd8d8644026 [Πρόσβαση 6 Μαΐου 2023]). Σήμερα, έχει επικρατήσει το μοντέλο της προγραμματικής διαφήμισης, το οποίο στηρίζεται στην αγοραπωλησία διαδικτυακών διαφημιστικών μηνυμάτων και χώρου μέσω αυτοματοποιημένων μηχανισμών, χωρίς ανθρώπινη παρέμβαση. Καρκατζούνης, Β. και Μήτρου, Λ. (2020) 'Online διαφήμιση και προστασία προσωπικών δεδομένων', *ΔiMEE*, 1/2020, σ. 7.

[388] Η Αμερικανίδα συγγραφέας Shoshanna Zuboff επινόησε τον όρο «καπιταλισμός της επιτήρησης» (surveillance capitalism) για να περιγράψει το επιχειρηματικό μοντέλο εμπορευματοποίησης των προσωπικών δεδομένων των χρηστών από τους τεχνολογικούς κολοσσούς του WEB 2.0, για τις «δωρεάν» υπηρεσίες των οποίων οι χρήστες «πληρώνουν» με τα προσωπικά δεδομένα τους. Για παράδειγμα, η Meta Platforms συγκεντρώνει καθημερινά πάνω από τέσσερα petabytes δεδομένων - ή αλλιώς δύο τρισεκατομμύρια (!) σελίδες τυπωμένου κειμένου - από την παρακολούθηση της επιγραμμικής δραστηριότητας των χρηστών της είτε στις ψηφιακές πλατφόρμες κοινωνικής δικτύωσης Facebook, WhatsApp και Instagram είτε σε τρίτες ιστοσελίδες και εφαρμογές στο κινητό τους, μέσω τεχνολογιών ιχνηλάτησης. Αργότερα, πουλάει τα προσωπικά δεδομένα τους σε τρίτες εταιρείες, κερδίζοντας ετησίως πάνω από 900 ευρώ για κάθε χρήστη από την πρακτική αυτή (βλ. Facebook pixel) και του δικτύου διαφημίσεών της (βλ. Martin, B. (2022), σ. 253-256).

Οι οικείοι πάροχοι θα μπορούν να παρακολουθούν πολλά περισσότερα από το πού κάνουν κλικ οι χρήστες[389]. Τα βιομετρικά δεδομένα και η συμπεριφορά των τελευταίων εντός του εικονικού κόσμου, θα υπόκεινται σε περαιτέρω επεξεργασία μέσω αλγορίθμων Τεχνητής Νοημοσύνης, ώστε, συνδυαζόμενα και με άλλα προσωπικά δεδομένα τους[390], να δημιουργούν συν τω χρόνω διεισδυτικά προφίλ χρήστη για τη στόχευση των υποκειμένων με απόλυτα εξατομικευμένο διαφημιστικό περιεχόμενο[391]. Οι πάροχοι θα γνωρίζουν με ακρίβεια πώς αντιδρούν ασυναίσθητα οι χρήστες σε εξωτερικά ερεθίσματα και τι αποκαλύπτουν αυτές οι αντιδράσεις για τις προτιμήσεις τους[392] (πχ. πόση ώρα «στέκεται» το βλέμμα τους σε ένα προϊόν[393];), πώς πράττουν και πώς αλληλεπιδρούν με το περιβάλλον τους (πχ. ποιες είναι οι συνήθειές τους και ο φιλικός τους κύκλος;), αλλά και ποια είναι η συναισθηματική τους κατάσταση κάθε στιγμή πλοήγησής τους στο Metaverse[394]. Άρα, θα είναι σε θέση όχι μόνο να προβλέψουν ποια διαφήμιση θα είναι η καταλληλότερη για να προβληθεί σε κάθε χρήστη μια δεδομένη χρονική στιγμή[395], αλλά εξίσου να δημιουργήσουν, με έντεχνο και αδιόρατο τρόπο, τις συνθήκες εκείνες υπό τις οποίες ο τελευταίος θα είναι πιο ευάλωτος να υποκύψει στο διαφημιζόμενο προϊόν ή τη χορηγούμενη υπηρεσία[396] [397]. Από την άλλη, οι έμποροι και διαφημιστές θα μπορούν να

---

[389] Rosenberg, L.B. (2022) 'Regulating the Metaverse, a Blueprint for the Future', L*ecture Notes in Computer Science (LNCS)*, 13445, σ. 263–272. Διαθέσιμο στο: https://doi.org/10.1007/978-3-031-15546-8_23, σ. 266.

[390] Με ήδη υπάρχουσες βάσεις δεδομένων ή/και με τα δεδομένα που οι χρήστες παρέχουν ενεργά στο Metaverse.

[391] Σύμφωνα με τις αιτήσεις διπλωμάτων ευρεσιτεχνίας της Meta Platforms, η τοποθέτηση διαφημίσεων στο Metaverse της εταιρείας θα λαμβάνει χώρα μέσω ενός συστήματος αυτοματοποιημένης δημοπρασίας, στο οποίο οι διαφημιζόμενοι θα υποβάλλουν προσφορές για να προωθήσουν διαφημιστικό περιεχόμενο εντός της πλατφόρμας. Τελικά, τον διαφημιστικό χώρο θα κερδίζει η διαφήμιση με την οποία ο χρήστης αναμένεται ότι θα αλληλεπιδράσει περισσότερο, εκτίμηση η οποία θα συνάγεται από τα προσωπικά δεδομένα του (βλ. Bloomberg, S. (2023) 'Political advertising in virtual reality', *SSRN Electronic Journal*. 23 Φεβρουαρίου. Διαθέσιμο στο: https://doi:10.2139/ssrn.4245908, σ. 28).

[392] Ό.π., Bloomberg, S. (2023), σ. 24.

[393] Ό.π., Rosenberg, L.B. (2022).

[394] Βλ. ό.π., Kim, Y. (2022), σ. 241 για VR.

[395] Ό.π., Bloomberg, S. (2023).

[396] Βλ. ό.π., Kim, Y. (2022).

[397] Έτσι, σε κάποιον που παρατηρείται να σταματάει τακτικά και να εστιάζει το βλέμμα του σε βιτρίνες εστιατορίων, η πλατφόρμα θα φροντίσει να προβάλει αυτόματα σχετικές διαφημίσεις φαγητού, χωρίς αυτός να έχει προηγουμένως αναζητήσει ενεργά σχετικές ιστοσελίδες καταστημάτων (βλ. ό.π. Murphy, S. et al. (2021)), ενώ στο οπτικό πεδίο της εικονικής πραγματικότητας κάποιου τρίτου, θα μπορούσε να εισάγει εκ των προτέρων ελκυστικά - βάσει των

μετρούν και να βελτιώνουν την αποδοτικότητα των διαφημίσεών τους, μέσω της ανάλυσης των βιομετρικών δεδομένων των χρηστών που θα παράγονται σε πραγματικό χρόνο κατά την προβολή αυτών και θα αντλούνται από τις συσκευές XR[398]. Σε κάθε περίπτωση, οι πάροχοι θα πλουτίζουν, πουλώντας τα προσωπικά δεδομένα των χρηστών και σε τρίτες εταιρείες (πχ. ασφαλιστικές) εκτός Metaverse[399], καθιστώντας τους χρήστες «διαφανείς» και ευάλωτους τόσο στον εικονικό, όσο και στον πραγματικό κόσμο.

Ασφαλώς, στη χειραγώγηση των χρηστών θα συμβάλει και ο τρόπος παρουσίασης των εικονικών διαφημίσεων στο Metaverse. Αν και δεν αποκλείεται η χρήση «διαφημίσεων προβολής» (display ads)[400], από τις οποίες θα προκύπτει εμφανώς ότι το προβαλλόμενο περιεχόμενο αποτελεί διαφήμιση, το εικονικό περιβάλλον του Metaverse θα στηριχθεί περισσότερο στο λεγόμενο "native advertising". Σε εξατομικευμένο, δηλαδή, διαφημιστικό περιεχόμενο που θα εγχέεται στον εικονικό κόσμο αθόρυβα και εν αγνοία του χρήστη, υπό μορφή προϊόντων, εμπειριών, αλλά και ανθρώπων που θα μοιάζουν - αλλά δεν θα είναι – ούτε οργανικό μέρος της εικονικής πλατφόρμας ούτε πραγματικοί άνθρωποι, αντίστοιχα[401]. Όταν οι χρήστες βλέπουν αυτοκίνητα μιας συγκεκριμένης μάρκας να κυκλοφορούν στους εικονικούς δρόμους ή συγκεκριμένα brands να κοσμούν τις εικονικές βιτρίνες, αυτό μάλλον θα οφείλεται στην Εικονική Τοποθέτηση Προϊόντος (Virtual Product Placements/VPPs)[402] που θα διενεργείται από την εικονική πλατφόρμα για λογαριασμό κάποιου διαφημιστή ή διαφημιζόμενου. Παράλληλα, θα έρχονται σε επαφή με «Εικονικούς Ανθρώπους» (Virtual People/Veeple), δηλαδή με πράκτορες λογισμικού Τεχνητής Νοημοσύνης που θα μοιάζουν, θα μιλούν (conversational AI) και θα φέρονται σαν αληθινοί χρήστες και θα έχουν ως στόχο να προωθήσουν υποσυνείδητα στους τελευταίους συγκεκριμένα αγαθά, υπηρεσίες ή ιδέες ενός τρίτου ενδιαφερόμενου μέρους[403]. Οι εικονικοί αυτοί εκπρόσωποι (spokespeople) θα προσομοιώνονται με τρόπο, ώστε να συγκεντρώνουν το σύνολο των εμφανισιακών και συμπεριφορικών εκείνων χαρακτηριστικών που είναι περισσότερο πιθανό να επηρεάσουν

προτιμήσεών του - τρόφιμα, με σκοπό αυτά να του αυξήσουν την όρεξη και στη συνέχεια να προβάλει μια στοχευμένη διαφήμιση ενός εστιατορίου (βλ. ό.π., Kim, Y. (2022)).

[398] Ό.π., Lumley, C. (2022) και ό.π., Aamir, O. (2022), σ. 24.

[399] Βλ. ό.π., Kim, Y. (2022), σ. 247, για την πολιτική απορρήτου της Oculus.

[400] Όπως πινακίδων (billboards), πανό (banners), αναδυόμενων παραθύρων (pop-ups), βίντεο (video commercials) (βλ. ό.π., Bloomberg, S. (2023), σ. 29) ή «πυλών» διαφημίσεων (portal ads) (βλ. ό.π., Bloomberg, S. (2023), σ. 25).

[401] Ό.π., Rosenberg, L.B. (2022), σ. 267.

[402] Ό.π.

[403] Ό.π.

τον υπό στόχευση χρήστη, βάσει προηγούμενων αλληλεπιδράσεων και ενεργειών του[404]. Σε κάθε περίπτωση, θα μπορούν να πείσουν με ευκολία τους χρήστες, έχοντας πρόσβαση σε δεδομένα του προφίλ τους και σε ψυχογραφικά δεδομένα που θα συνάγονται σε πραγματικό χρόνο από τις βιολογικές αντιδράσεις τους[405].

Όλα τα παραπάνω θα μπορούν να εφαρμοστούν και για την προώθηση πολιτικών προσώπων και ιδεών (πχ. ο χρήστης θα μπορεί να βλέπει το άβαταρ ενός υποψηφίου να τον χαιρετάει προσωπικά, καθώς περπατάει στο εικονικό πεζοδρόμιο[406]), ενώ αναμένεται να εμφανιστούν και *«εμβυθιστικά περιβάλλοντα προεκλογικής εκστρατείας» (immersive electioneering environments)*[407], δηλαδή πολιτικές εκδηλώσεις απόλυτα προσαρμοσμένες στο προφίλ του κάθε χρήστη, για την αποτελεσματική στόχευση του εκλογικού κοινού, εν είδει ενός προωθημένου Cambridge Analytica.

Το δυστοπικό Metaverse θα αποτελέσει ένα περιβάλλον διαιώνισης και ενίσχυσης των προκαταλήψεων και των διακρίσεων μεταξύ της κοινότητας των χρηστών του. Όπως όλα τα αλγοριθμικά συστήματα[408], έτσι και τα εργαλεία Τεχνητής Νοημοσύνης που θα ενσωματωθούν και θα επιτρέψουν τη λειτουργία του Metaverse, θα εμπεδώνουν προκαταλήψεις και στερεότυπα (biased AI) από τα οποία θα εμφορείται ο ανθρώπινος νους που θα τα σχεδιάσει, προγραμματίσει και εκπαιδεύσει. Ήδη προκαλεί ανησυχία το γεγονός ότι η πλειονότητα των κατασκευαστών του Metaverse ανήκουν σε μια ομοιογενή κοινότητα λευκών ανδρών[409]. Εκτός αυτού, έρευνες του UCL (University College of London) έδειξαν ότι η αλληλεπίδραση ανθρώπων και Τεχνητής Νοημοσύνης δημιουργεί έναν φαύλο κύκλο *("feedback loop")*, εντός του οποίου προκατειλημμένοι άνθρωποι αναπτύσσουν μεροληπτικά αλγοριθμικά συστήματα, τα μεροληπτικά αυτά αλγοριθμικά συστήματα με τη σειρά τους

---

[404] Ό.π., σ. 268.

[405] Ό.π.

[406] Ό.π., Bloomberg, S. (2023), σ. 31.

[407] Ό.π.

[408] Για παράδειγμα, ο αλγόριθμος Apple Card της Apple αποδείχθηκε ότι ενίσχυε διακρίσεις με βάση το φύλο (βλ. Hamilton, I. A. (2019) 'Apple cofounder Steve Wozniak says Apple Card offered his wife a lower credit limit', *Insider*, 11 Νοεμβρίου. Διαθέσιμο στο: https://www.businessinsider.com/apple-card-sexism-steve-wozniak-2019-11?IR=T [Πρόσβαση 6 Μαΐου 2023]), ενώ ο αλγόριθμος COMPAS της Equivant (τέως Northpointe) με βάση τη φυλή (βλ. Datatron Blog (2022) *Real-life Examples of Discriminating Artificial Intelligence*. Διαθέσιμο στο: https://datatron.com/real-life-examples-of-discriminating-artificial-intelligence/ [Πρόσβαση 6 Μαΐου 2023]).

[409] Ό.π., Kalpokas, I. and Kalpokienė, J. (2023), σ. 66.

διαστρεβλώνουν ακόμη περισσότερο την ανθρώπινη κρίση και ούτω καθεξής[410]. Επομένως, η αναγκαία αλληλεπίδραση μεταξύ χρηστών και αλγορίθμων στο εικονικό περιβάλλον είναι πολύ πιθανό να ωθήσει σε ενίσχυση των ήδη υπαρχουσών προκαταλήψεων, σε ριζοσπαστικοποίηση των απόψεων και σε διάχυση της παραπληροφόρησης μεταξύ των χρηστών του και αντίστροφα, σε περαιτέρω διόγκωση αυτών των φαινομένων από τα αλγοριθμικά εργαλεία. Τα εξαγόμενα προσωπικά δεδομένα των χρηστών και το ατομικό προφίλ που θα καταρτίζεται δυνάμει αυτών για καθέναν τους, ενδέχεται, λοιπόν, να τους εκθέσει σε διαφόρων ειδών διακρίσεις, υπό μορφή αυτοματοποιημένων μεροληπτικών αποφάσεων που θα λαμβάνονται ερήμην τους και για λογαριασμό τους από έξυπνα συστήματα. Οι χρήστες πιθανόν να στερούνται την πρόσβαση σε εικονικούς χώρους, υπηρεσίες ή ευκαιρίες, λόγω του φύλου, της ηλικίας, της φυλής, του σεξουαλικού προσανατολισμού, των πολιτικών και θρησκευτικών πεποιθήσεων ή της κατάστασης της υγείας τους. Σε πολλές περιπτώσεις, η κατάρτιση του προφίλ τους ενδέχεται να είναι και εσφαλμένη[411], βασιζόμενη σε αποκλίνοντα χαρακτηριστικά ή συμπεριφορές που υιοθετούν εντός του εικονικού κόσμου και τα οποία παρά ταύτα θα χρησιμεύουν για την αλγοριθμική λήψη αποφάσεων που τους αφορούν ή τους επηρεάζουν.

Στο πλαίσιο αυτό, εκτιμάται ότι μία πρακτική λύση για την αποτροπή των κινδύνων της συμπεριφορικής διαφήμισης στο Metaverse είναι η μετατόπιση από επιχειρηματικά μοντέλα που βασίζονται σε διαφημίσεις (ad-based) σε επιχειρηματικά μοντέλα που βασίζονται σε συνδρομές (subscription-based)[412]. Ωστόσο, κανείς δεν εγγυάται ότι οι χρήστες θα είναι πρόθυμοι να πληρώσουν εξ αρχής για την παροχή των συναφών υπηρεσιών. Αυτό που αναμένεται, λοιπόν, να συμβεί είναι να τους παρέχεται η δυνατότητα να επιλέξουν μεταξύ των δύο. Η επιτυχία των οικείων παρόχων θα είναι να δελεάσουν τους χρήστες αρχικά να επιλέξουν τη (δωρεάν) εικονική πλατφόρμα τους και στη συνέχεια να μείνουν σε αυτή, ωθώντας τους παράλληλα στη συνδρομητική έκδοσή της[413]. Για σκοπούς όμως συμμόρφωσης προς τον ΓΚΠΔ, η ανάκληση της συγκατάθεσης όσων έχουν επιλέξει τη δωρεάν έκδοση για την επεξεργασία των προσωπικών δεδομένων

[410] Ό.π., Anidjar, L.Y., Packin, N.G. and Panezi, A. (2023), σ. 21.

[411] Βλ. ό.π., Kim, Y. (2022), σ. 246, για VR.

[412] Ό.π., Rosenberg, L.B. (2022), σ. 268.

[413] Ό.π., Kalpokas, I. and Kalpokienė, J. (2023), σ. 59.

τους για σκοπούς διαφήμισης, θα πρέπει να τους επιτρέπει να συνεχίσουν να χρησιμοποιούν τη δωρεάν αυτή έκδοση, χωρίς στοχευμένες πια διαφημίσεις[414].

Σε κάθε περίπτωση, το άρθρο 21 παρ. 2 ΓΚΠΔ χορηγεί στο υποκείμενο το δικαίωμα να εναντιωθεί ανά πάσα στιγμή στην επεξεργασία των προσωπικών του δεδομένων που διενεργείται για σκοπούς απευθείας εμπορικής προώθησης, συμπεριλαμβανομένης της σχετικής με αυτήν κατάρτισης προφίλ, ενώ η παρ. 3 του ίδιου άρθρου ορίζει ότι όταν το υποκείμενο αντιτάσσεται, τα δεδομένα του δεν υποβάλλονται πλέον σε επεξεργασία για τέτοιους σκοπούς. Το εν λόγω δικαίωμα πρέπει, σύμφωνα με την παρ. 4, να γνωστοποιείται στο υποκείμενο και να περιγράφεται με σαφήνεια και χωριστά από οποιαδήποτε άλλη πληροφορία. Συνεπώς, οι χρήστες του Metaverse θα πρέπει να μπορούν να εναντιωθούν οποτεδήποτε στην επεξεργασία των προσωπικών δεδομένων τους που θα διενεργείται για τη στόχευσή τους με διαφημιστικό περιεχόμενο, ανεξαρτήτως της νόμιμης βάσης που θα επικαλείται κάθε φορά ο υπεύθυνος επεξεργασίας. Προτείνεται να αποσαφηνιστεί μέσω Κατευθυντήριων γραμμών το περιεχόμενο του εν λόγω δικαιώματος στο Metaverse και να περιληφθούν στην έννοια της απευθείας εμπορικής προώθησης στην οποία θα μπορούν να εναντιωθούν τα υποκείμενα και οι περιπτώσεις πολιτικής προώθησης.

Από την άλλη, το άρθρο 22 παρ. 1 ΓΚΠΔ θεσπίζει τη γενική απαγόρευση υπαγωγής του υποκειμένου σε αποφάσεις που λαμβάνονται *αποκλειστικά* με αυτοματοποιημένα μέσα, συμπεριλαμβανομένης της κατάρτισης προφίλ, και οι οποίες παράγουν έννομα αποτελέσματα που το αφορούν[415] ή το επηρεάζουν ουσιωδώς με όμοιο τρόπο[416], εκτός κι αν

---

[414] «*Ο υπεύθυνος επεξεργασίας θα πρέπει να αποδείξει ότι το υποκείμενο των δεδομένων μπορεί να αρνηθεί ή να αποσύρει τη συγκατάθεσή του χωρίς να ζημιωθεί (αιτιολογική σκέψη 42). Για παράδειγμα, ο υπεύθυνος επεξεργασίας θα πρέπει να αποδείξει ότι η ανάκληση της συγκατάθεσης δεν συνεπάγεται κανένα κόστος για το υποκείμενο των δεδομένων και, επομένως, κανένα σαφές μειονέκτημα για εκείνον που ανακαλεί τη συγκατάθεσή του* (βλ. ό.π., Κατευθυντήριες 5/2020, σ. 15).

[415] Πχ. ακύρωση μιας σύμβασης, αποκλεισμός από κοινωνική παροχή που χορηγείται βάσει νόμου, άρνηση εισδοχής σε μια χώρα κ.ο.κ. (βλ. Ομάδα προστασίας δεδομένων του άρθρου 29, Κατευθυντήριες γραμμές για την αυτοματοποιημένη λήψη αποφάσεων και την κατάρτιση προφίλ για τους σκοπούς του κανονισμού 2016/679, της 6ης Φεβρουαρίου 2018. Διαθέσιμο στο: https://ec.europa.eu/newsroom/article29/items/612053/en, σ. 25).

[416] Πχ. αποφάσεις που επηρεάζουν την οικονομική κατάσταση ενός φυσικού προσώπου, που έχουν ως αποτέλεσμα τον αποκλεισμό του από μια ευκαιρία απασχόλησης ή τη διαμόρφωση έντονα μειονεκτικής θέσης για το εν λόγω φυσικό πρόσωπο, που επηρεάζουν τη δυνατότητα πρόσβασής του σε υπηρεσίες υγείας ή στην εκπαίδευση κ.ο.κ. (βλ. ό.π., σ. 26).

πληρούται μία εκ των προϋποθέσεων της παρ. 2[417], μεταξύ των οποίων συγκαταλέγεται και η ανάγκη για τη σύναψη ή την εκτέλεση σύμβασης μεταξύ του υποκειμένου και του υπευθύνου επεξεργασίας[418]. Είναι δεδομένο ότι στο εικονικό περιβάλλον του Metaverse, ένα μεγάλο ποσοστό των απολύτως αυτοματοποιημένων αποφάσεων θα λαμβάνεται με τέτοιο τρόπο, λόγω της ανάγκης για σύναψη ή εκτέλεση σύμβασης μεταξύ των χρηστών του και του εκάστοτε υπευθύνου επεξεργασίας. Για παράδειγμα, μια εταιρεία που επιθυμεί να προσλάβει υπαλληλικό προσωπικό μέσω του Metaverse, ενδέχεται να δεχτεί χιλιάδες αιτήσεις από υποψηφίους εργαζομένους-χρήστες ανά τον κόσμο, οι οποίες θα μπορούν να περιοριστούν σε έναν κατάλογο επίλεκτων υποψηφίων μόνο μέσω της αλγοριθμικής επεξεργασίας τους. Κατά τον ίδιο τρόπο, δεν μπορεί να αποκλειστεί (εφόσον υπάρχει νόμιμος λόγος) η αυτοματοποιημένη κατάρτιση προφίλ και η δυνάμει αυτής αυτοματοποιημένη προβολή διαφημιστικού περιεχομένου στο Metaverse, καθώς η φύση της σύμβασης του χρήστη με τον πάροχο της εικονικής πλατφόρμας δεν επιτρέπει την εκτέλεσή της για τον σκοπό αυτό με μη αυτοματοποιημένα μέσα.

Ο ΓΚΠΔ θεσπίζει εχέγγυα προστασίας των υποκειμένων για αυτές τις εξαιρέσεις. Ειδικότερα, τα άρθρα 13 παρ. 2 στ. στ' και 14 παρ. 2 στ. ζ' επιβάλλουν στον υπεύθυνο την ενημέρωση του υποκειμένου για την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ, σύμφωνα με τα άρθρα 22 παρ. 1 και 4 και, τουλάχιστον στις περιπτώσεις αυτές, σημαντικές πληροφορίες σχετικά με τη λογική που ακολουθείται, καθώς και τη σημασία και τις προβλεπόμενες συνέπειες της εν λόγω επεξεργασίας για το υποκείμενο των δεδομένων. Το ζήτημα της διαφάνειας επανέρχεται εδώ και οι υπεύθυνοι επεξεργασίας στο Metaverse οφείλουν να ενημερώνουν επαρκώς τα υποκείμενα για οποιαδήποτε αλγοριθμική λήψη απόφασης, ιδίως για τα αποφασιστικά κριτήρια που θα οδηγούν στη λήψη της (είδος, πηγή και συνάφεια πληροφοριών), αλλά και να τους παρέχουν απτά, κατανοητά παραδείγματα που να απεικονίζουν τις συνέπειες της σκοπούμενης ή μελλοντικής επεξεργασίας[419]. Περαιτέρω, σύμφωνα με την παρ. 3 του

[417] Όσον αφορά στα ευαίσθητα προσωπικά δεδομένα, θεσπίζεται ως πρόσθετη προϋπόθεση η λήψη της συναίνεσης των υποκειμένων για την αυτοματοποιημένη λήψη αποφάσεων ή η επεξεργασία δυνάμει του άρθρου 9 παρ. 2 στ. ζ ΓΚΠΔ.

[418] Ο υπεύθυνος επεξεργασίας θα πρέπει να μπορεί να αποδείξει ότι δεν είναι δυνατόν να ληφθούν λιγότερο παρεμβατικά μέτρα για την ιδιωτικότητα του υποκειμένου (βλ. ό.π., Κατευθυντήριες γραμμές για την αυτοματοποιημένη λήψη αποφάσεων και την κατάρτιση προφίλ για τους σκοπούς του κανονισμού 2016/679, σ. 28).

[419] Ό.π., σ. 30-31.

άρθρου 22, ακόμη και σε αυτές τις περιπτώσεις, ο υπεύθυνος επεξεργασίας οφείλει να λαμβάνει κατάλληλα μέτρα για την προστασία των δικαιωμάτων και ελευθεριών των υποκειμένων, τουλάχιστον να εξασφαλίζει την ανθρώπινη παρέμβαση από την πλευρά του, το δικαίωμα ακροάσεως του υποκειμένου και τη δυνατότητα ανατροπής των εν λόγω αποφάσεων. Η Ομάδα προστασίας δεδομένων του άρθρου 29, στις οικείες Κατευθυντήριες γραμμές της[420], τονίζει ότι η ανθρώπινη παρέμβαση πρέπει να είναι ουσιαστική, δηλαδή να διενεργείται από άτομο το οποίο έχει την εξουσιοδότηση και αρμοδιότητα να μεταβάλει την απόφαση. Στο πλαίσιο αυτό, υποστηρίζεται ότι κάθε οντότητα που δραστηριοποιείται στο Metaverse θα πρέπει να δημιουργήσει ένα ανεξάρτητο -και με αυξημένες υποχρεώσεις δημοσιότητας- όργανο για την επίλυση των διαφορών της με τους χρήστες[421], μεταξύ άλλων για την αμφισβήτηση των αυτοματοποιημένων μεροληπτικών αποφάσεων που λαμβάνονται από τους οικείους παρόχους και επηρεάζουν την έννομη κατάσταση του χρήστη ή παρουσιάζουν ισοδύναμες επιπτώσεις στη ζωή του εντός και εκτός Metaverse. Οπωσδήποτε, η έννοια της επαρκούς ανθρώπινης παρέμβασης κατά την αναθεώρηση των αυτοματοποιημένων αποφάσεων που θα λαμβάνονται στο Metaverse είναι ανάγκη να εξειδικευθεί ρυθμιστικά (ποια εχέγγυα και ποιες προϋποθέσεις θα πρέπει να πληρούν τα πρόσωπα ή τα όργανα που θα κρίνουν επί των ενστάσεων των χρηστών;).

Καθώς όμως ο όγκος των αποκλειστικά αυτοματοποιημένων αποφάσεων που θα λαμβάνονται στο Metaverse ενδέχεται να είναι μη διαχειρίσιμος, δεν μπορεί να αναμένεται από τους χρήστες να αιτούνται την επανεξέταση όσων τέτοιων αποφάσεων θεωρούν ότι τους έχουν πλήξει. Επιπλέον, πολλές από τις αποφάσεις αυτές ενδέχεται να μην πληρούν το κριτήριο της έννομης ή έστω ουσιώδους επιρροής των χρηστών (πχ. η απαγόρευση της εισόδου σε έναν εικονικό χώρο μπορεί να θεωρηθεί ότι εμπίπτει στο πεδίο της νομοθετικής διάταξης;). Για το λόγο αυτό, πρέπει να δοθεί προτεραιότητα στην ανάπτυξη αμερόληπτων αλγοριθμικών συστημάτων από τους παρόχους, μέσω της απαραίτητης καθοδήγησης εκ μέρους των εποπτικών αρχών για την αφαίρεση των μεροληπτικών δεδομένων από τα αντίστοιχα αλγοριθμικά συστήματα[422] (πχ. με τη χρήση συνθετικών δεδομένων-synthetic data για τον εμπλουτισμό των συναφών βάσεων εκπαιδευτικών δεδομένων[423]).

---

[420] Ό.π., σ. 25.

[421] Ό.π., Anidjar, L.Y., Packin, N.G. and Panezi, A. (2023), σ. 49.

[422] Ό.π., Anidjar, L.Y., Packin, N.G. and Panezi, A. (2023), σ. 47.

[423] Ό.π.

Στο Metaverse ενδέχεται να εφαρμοστούν και άλλα δύο νομοθετήματα ενωσιακού δικαίου, ο Κανονισμός DSA[424] και η Πρόταση Κανονισμού για την Τεχνητή Νοημοσύνη (διεθνώς και εφεξής "AI Act")[425], αφού υιοθετηθεί. Ο Κανονισμός DSA περιέχει διατάξεις για τη διαφάνεια και λογοδοσία των παρόχων επιγραμμικών πλατφορμών αναφορικά με τις προβαλλόμενες επιγραμμικές διαφημίσεις. Η AI Act περιλαμβάνει διατάξεις για την κατηγοριοποίηση των συστημάτων Τεχνητής Νοημοσύνης με βάση τον κίνδυνο και όσον αφορά στα συστήματα υψηλού κινδύνου, θεσπίζει αυστηρές υποχρεώσεις διασφάλισης της ποιότητας των εισαγόμενων σε αυτά δεδομένων, ούτως ώστε να μην αποτελούν πηγή διακρίσεων, και υποχρεώσεις λογοδοσίας, διαφάνειας, επαρκούς πληροφόρησης των χρηστών, ανθρώπινης εποπτείας, ακρίβειας, στιβαρότητας, κυβερνοασφάλειας κλπ.

Παρόλα αυτά, τα ανωτέρω νομοθετήματα δεν επαρκούν για την προστασία των προσωπικών δεδομένων των υποκειμένων στο Metaverse. Ο ΓΚΠΔ, ως αρμόδια ενωσιακή νομοθεσία - με ευρύτερο, μάλιστα, εδαφικό πεδίο εφαρμογής -, πρέπει να ερμηνευθεί κατάλληλα -ενώ απευθύνονται και εκκλήσεις για την τροποποίησή του[426]-, με σκοπό να ανταποκριθεί στις πρωτοφανείς προκλήσεις που θα θέσει η συγκέντρωση και περαιτέρω επεξεργασία δεδομένων εξαγόμενων κατά την ασυνείδητη συμπεριφορά των χρηστών, και στο πλαίσιο της συνεχούς συναναστροφής τους με αλγοριθμικά συστήματα Τεχνητής Νοημοσύνης. Στο πλαίσιο αυτό, γνώμη της γράφουσας είναι ότι ο ΓΚΠΔ θα ήταν σκόπιμο να τροποποιηθεί, ώστε να περιορίζεται αισθητά η κατάρτιση προφίλ που θα βασίζεται στην παρακολούθηση της συμπεριφοράς των χρηστών σε εικονικά περιβάλλοντα.

3.5. Διαβιβάσεις προσωπικών δεδομένων

3.5.1. Φορητότητα προσωπικών δεδομένων και διαλειτουργικότητα

Η φορητότητα των προσωπικών δεδομένων των χρηστών από τη μία πλατφόρμα Metaverse στην άλλη και η διαλειτουργικότητα των χρησιμοποιούμενων μορφοτύπων θα αποτελέσει σημείο κλειδί για την κατάργηση των ιδιωτικών μονοπωλίων και των σιλό

[424] Κανονισμός (ΕΕ) 2022/2065 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 19ης Οκτωβρίου 2022, σχετικά με την ενιαία αγορά ψηφιακών υπηρεσιών και την τροποποίηση της οδηγίας 2000/31/εκ (πράξη για τις ψηφιακές υπηρεσίες).

[425] Πρόταση Κανονισμού (ΕΕ) του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 21ης Απριλίου 2022, για τη θέσπιση εναρμονισμένων κανόνων σχετικά με την τεχνητή νοημοσύνη (Πράξη για την Τεχνητή Νοημοσύνη) και την τροποποίηση ορισμένων νομοθετικών πράξεων της Ένωσης.

[426] Ό.π., European Parliamentary Research Service (EPRS) (2022), σ. 6.

δεδομένων (data silos) που μαστίζουν το WEB 2.0, διασφαλίζοντας σε μικρότερες πλατφόρμες μεγαλύτερες επιχειρηματικές ευκαιρίες[427] και στους χρήστες διευρυμένο έλεγχο επί των δεδομένων τους.

Ο ΓΚΠΔ χορηγεί στα υποκείμενα το δικαίωμα φορητότητας, δηλαδή το δικαίωμα να λαμβάνουν όσα προσωπικά δεδομένα έχουν παράσχει[428] στον υπεύθυνο επεξεργασίας σε δομημένη, κοινώς χρησιμοποιούμενη και μηχανικά αναγνώσιμη μορφή και να διαβιβάζουν αυτά χωρίς αντίρρηση από τον τελευταίο σε άλλον υπεύθυνο επεξεργασίας[429] της επιλογής τους[430] (άρθρο 20). Παρόλα αυτά, το σχετικό δικαίωμα απονέμεται στα υποκείμενα μόνο εφόσον τα προσωπικά δεδομένα τους έχουν υποστεί αυτοματοποιημένη επεξεργασία και μόνο επί τη (νόμιμη) βάσει της συγκατάθεσης (άρθρα 6 παρ. 1 στοιχ. α' και 9 παρ. 2 στοιχ. α') ή της σύμβασης (άρθρο 6 παρ. 1 στοιχ. β'). Επιπλέον, αν και ο ΓΚΠΔ ενθαρρύνει την ανάπτυξη διαλειτουργικών μορφοτύπων για τη διευκόλυνση της ουσιαστικής άσκησης του δικαιώματος στη φορητότητα[431], δεν επιβάλλει ειδική υποχρέωση στους υπεύθυνους επεξεργασίας για τη διασφάλιση της διαλειτουργικότητας.

Στο Metaverse, όμως, προβλέπεται ότι λίγες θα είναι οι εταιρείες εκείνες που θα είναι δεκτικές στη δημιουργία διαλειτουργικών μορφοτύπων[432]. Άλλωστε, κύριος στόχος των οικείων παρόχων είναι να δημιουργήσουν εικονικούς κόσμους που θα προσφέρουν στους χρήστες μια μεγάλη γκάμα δυνατοτήτων και εμπειριών, ώστε να μη χρειαστεί να

---

[427] Ό.π., Mangada Real de Asúa, E. et al. (2022), σ. 18.

[428] Αφορά τα προσωπικά δεδομένα που τα υποκείμενα παρέχουν συνειδητά και ενεργητικά, αλλά και όσα προσωπικά δεδομένα παράγονται και παρατηρούνται από τη δραστηριότητά τους κατά τη χρήση της υπηρεσίας. Αντιθέτως, δεν περιλαμβάνονται δεδομένα που συνάγονται από τα δεδομένα που παρέχει το υποκείμενο, όπως για παράδειγμα το προφίλ χρήστη που καταρτίζει ο υπεύθυνος (βλ. Ομάδα προστασίας δεδομένων του άρθρου 29, Κατευθυντήριες γραμμές σχετικά με το δικαίωμα στη φορητότητα των δεδομένων, της 5ης Απριλίου 2017. Διαθέσιμο στο: https://www.lawspot.gr/sites/default/files/misc/misc_legal/wp242rev01_el.pdf, σ. 12).

[429] Επίσης, σύμφωνα με το άρθρο 20 παρ. 2 ΓΚΠΔ, το υποκείμενο των δεδομένων δικαιούται να ζητήσει την απευθείας διαβίβαση αυτών από τον έναν υπεύθυνο επεξεργασίας στον άλλον, αν αυτό είναι τεχνικά εφικτό.

[430] Ο υπεύθυνος επεξεργασίας πρέπει να επαληθεύει την ταυτότητα του υποκειμένου πριν την ικανοποίηση του αιτήματός του και να εξασφαλίζει ότι τα δεδομένα που μεταφέρονται είναι ακριβή και επικαιροποιημένα, σύμφωνα με την αρχή της ακρίβειας (άρθρο 5 παρ. 1 στοιχ. δ' ΓΚΠΔ), ενώ ο λαμβάνων υπεύθυνος επεξεργασίας πρέπει να διασφαλίζει ότι τα προσωπικά δεδομένα είναι συναφή και αναγκαία για τη διενεργούμενη από αυτόν επεξεργασία, ότι το υποκείμενο έχει ενημερωθεί κατάλληλα για το σκοπό αυτής και ότι έχουν τηρηθεί όλες οι αρχές προστασίας που επιτάσσει ο ΓΚΠΔ.

[431] Βλ. αιτιολογική σκέψη 68 εδ. β' ΓΚΠΔ.

[432] Ό.π., Kalpokas, I. and Kalpokienė, J. (2023), σ. 92. και ό.π., Floridi, L. (2022), σ. 4.

αναζητήσουν τίποτα εκτός πλατφόρμας[433]. Είναι αναμενόμενο ότι υπό αυτές τις συνθήκες, οι χρήστες δεν θα πιέσουν προς την κατεύθυνση της διαλειτουργικότητας[434]. Επίσης, στην περίπτωση που συνυπάρξουν εντέλει διαφόρων ειδών πλατφόρμες Metaverse και ζητείται η μεταφορά των δεδομένων του χρήστη από τη μία στην άλλη, είναι πιθανό προβλήματα τεχνικής φύσεως να αποτρέψουν επί της ουσίας τη φορητότητα.

Στο πλαίσιο αυτό, ο πολύ σημαντικός για το Metaverse περιορισμός των ιδιωτικών μονοπωλίων και συνεπώς, η αποτελεσματική προστασία της αυτονομίας των χρηστών, θα επιτευχθεί μόνο αν οι πάροχοι υποχρεωθούν νομοθετικά να ρυθμίσουν by design και by default τη δυνατότητα των υποκειμένων να αλλάζουν εύκολα και ανέξοδα πάροχο και να μεταφέρουν απρόσκοπτα προσωπικά δεδομένα μεταξύ των διαφορετικών πλατφορμών, αναπτύσσοντας και υιοθετώντας διαλειτουργικά πρότυπα και πρωτόκολλα που εγγυώνται τη φορητότητα. Γνωρίζοντας ότι δεν θα ρισκάρουν να χάσουν προσωπικά δεδομένα τους ή ότι δεν θα χρειαστεί να εισάγουν από την αρχή το σύνολο όσων από αυτά έχουν παράσχει σε προηγούμενο πάροχο (πχ. λίστες επαφών, αρχεία, αποθηκευμένες ρυθμίσεις, όπως ρυθμίσεις γλώσσας κ.ο.κ.), οι χρήστες θα μπορούν να επιλέξουν ελεύθερα και χωρίς ενδοιασμούς αν θα μείνουν ή θα εγκαταλείψουν την πλατφόρμα που ήδη χρησιμοποιούν. Λέγεται, μάλιστα, πως αυτό θα καταστεί εφικτό μόνο αν το δικαίωμα στη φορητότητα τους χορηγείται ανεξαρτήτως της νομικής βάσης επεξεργασίας που θα χρησιμοποιείται από κάθε πάροχο, σε αντίθεση με τα έως τώρα προβλεπόμενα[435].

Καθώς όμως το Metaverse θα αποτελέσει ένα περίπλοκο δίκτυο αλληλεπιδράσεων μεταξύ παρόχων πρόσβασης, χρηστών και τρίτων μερών, ενδέχεται να αποβεί εξαιρετικά δύσκολο για τα υποκείμενα να αναγνωρίσουν ποιοι «κατέχουν» στην πραγματικότητα τα δεδομένα τους και ποιοι ευθύνονται τελικά για την επεξεργασία τους, ώστε να ασκήσουν έναντι αυτών το δικαίωμα στη φορητότητα. Από την άλλη, οι πολλαπλές διαβιβάσεις προσωπικών δεδομένων μεταξύ των παρόχων εγκυμονούν αυξημένους κινδύνους για την ασφάλειά τους[436], ενώ δεν μπορεί να αποκλειστεί ούτε το φαινόμενο της απώλειας της αξίας τους (value loss), όταν μεταφέρονται από τη μία πλατφόρμα Metaverse στην άλλη[437].

---

[433] Ό.π., Kalpokas, I. and Kalpokienė, J. (2023), σ. 90.

[434] Ό.π., Kalpokas, I. and Kalpokienė, J. (2023), σ. 92.

[435] Ό.π., Knibbeler, D., Mohrmann, M. and Zadeh, S. (2022).

[436] Ό.π., Kalpokas, I. and Kalpokienė, J. (2023), σ. 100 και ό.π., Κουσουνή-Πανταζοπούλου, Α. (2023), σ. 381.

[437] Ό.π., Mangada Real de Asúa, E. et al. (2022), σ. 18.

Εν πάση περιπτώσει, όμως, η διασφάλιση της φορητότητας, της διαλειτουργικότητας και η λήψη μέτρων για την ασφάλεια των υπό διαβίβαση δεδομένων φαίνεται να αποτελεί την πιο αξιόπιστη προσέγγιση[438].

3.5.2. Διαβίβαση προσωπικών δεδομένων εκτός ΕΕ

Η διαβίβαση προσωπικών δεδομένων σε τρίτες χώρες και διεθνείς οργανισμούς υπό το ισχύον νομοθετικό καθεστώς υπόκειται σε αυστηρούς κανόνες, ώστε να διασφαλίζεται ότι το επίπεδο προστασίας των υποκειμένων που εγγυάται ο ΓΚΠΔ δεν υπονομεύεται.

Νόμιμη βάση για την εν λόγω διαβίβαση αποτελούν οι αποφάσεις επάρκειας της Ευρωπαϊκής Επιτροπής (άρθρο 45 ΓΚΠΔ), τις οποίες εκδίδει εφόσον κρίνει ότι το τρίτο κράτος ή ο διεθνής οργανισμός παρέχει ικανοποιητικό επίπεδο προστασίας προσωπικών δεδομένων. Ελλείψει απόφασης επάρκειας, ο υπεύθυνος επεξεργασίας ή εκτελών μπορεί να διαβιβάσει νομίμως τα προσωπικά δεδομένα, εφόσον παρέχει κατάλληλες εγγυήσεις σύμφωνα με το άρθρο 46 ΓΚΠΔ (πχ. δεσμευτικοί εταιρικοί κανόνες – Binding Corporate Rules/BCR, τυποποιημένες συμβατικές ρήτρες, εγκεκριμένος κώδικας δεοντολογίας, εγκεκριμένος κώδικας πιστοποίησης κλπ.) και υπό τον όρο ότι υφίστανται εκτελεστά δικαιώματα και αποτελεσματικά ένδικα μέσα προστασίας των υποκειμένων στην τρίτη αυτή χώρα ή τον διεθνή οργανισμό. Ως ύστατη λύση για τη διαβίβαση εφαρμόζονται οι παρεκκλίσεις του άρθρου 49 ΓΚΠΔ, που αφορούν σε ειδικές περιπτώσεις (πχ. το υποκείμενο συναινεί στη διαβίβαση, κατόπιν σχετικής ενημέρωσής του για τους πιθανούς κινδύνους από την έλλειψη των μηχανισμών των άρθρων 46 και 49 ΓΚΠΔ κλπ.).

Αναφορικά με τη διαβίβαση προσωπικών δεδομένων από την ΕΕ στις ΗΠΑ, σε συνέχεια της απόφασης Schrems I[439] που κατήργησε την απόφαση 2000/520/ΕΚ[440] της Ευρωπαϊκής Επιτροπής σχετικά με την επάρκεια της παρεχόμενης προστασίας από τις αρχές ασφαλούς λιμένα για την προστασία της ιδιωτικής ζωής και τις συναφείς συχνές ερωτήσεις που εκδίδονταν από το Υπουργείο Εμπορίου των ΗΠΑ (Safe Harbor), η απόφαση

---

[438] Ό.π.

[439] Απόφαση ΔΕΕ C-362/14, Maximillian Schrems, της 6ης Οκτωβρίου 2015. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:62014CJ0362&from=en.

[440] Απόφαση (ΕΚ) 2000/520 της Ευρωπαϊκής Επιτροπής, της 26ης Ιουλίου 2000, βάσει της οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την επάρκεια της προστασίας που παρέχεται από τις αρχές ασφαλούς λιμένα για την προστασία της ιδιωτικής ζωής και τις συναφείς συχνές ερωτήσεις που εκδίδονται από το Υπουργείο Εμπορίου των ΗΠΑ. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32000D0520.

Schrems II[441] κατήργησε την απόφαση 2016/1250/ΕΕ[442] της Ευρωπαϊκής Επιτροπής σχετικά με την επάρκεια της παρεχόμενης προστασίας από την ασπίδα προστασίας της ιδιωτικής ζωής μεταξύ ΕΕ-ΗΠΑ (Privacy Shield)[443]. Σε αμφότερες τις περιπτώσεις, το ΔΕΕ έκρινε πως το νομοθετικό καθεστώς των ΗΠΑ δεν παρείχε τα κατάλληλα εχέγγυα - ούτε σε επίπεδο νόμων ούτε σε επίπεδο διαδικασιών - για την προστασία των προσωπικών δεδομένων που διαβιβάζονταν από την ΕΕ στις ΗΠΑ.

Την 25η Μαρτίου 2022, η ΕΕ και οι ΗΠΑ κατέληξαν σε κατ' αρχήν συμφωνία για ένα νέο πλαίσιο προστασίας όσον αφορά στις ροές δεδομένων ΕΕ-ΗΠΑ και την 7η Οκτωβρίου 2022, ο Πρόεδρος Joseph Biden υπέγραψε εκτελεστικό διάταγμα για «την ενίσχυση των εγγυήσεων για τις δραστηριότητες πληροφοριών των Ηνωμένων Πολιτειών» ("Enhancing Safeguards for United States Signals Intelligence Activities")[444]. Επί της ουσίας, το εν λόγω εκτελεστικό διάταγμα και οι συνοδευτικοί αυτού Κανονισμοί του αμερικανικού Υπουργείου Δικαιοσύνης υλοποιούν τη συμφωνία του Μαρτίου[445]. Επόμενο διαδικαστικό στάδιο είναι η έκδοση απόφασης επάρκειας από την Ευρωπαϊκή Επιτροπή, επί του σχεδίου της οποίας θα πρέπει να γνωμοδοτήσει το ΕΣΠΔ και αυτό να εγκριθεί από ειδική επιτροπή εκπροσώπων των κρατών – μελών[446]. Το Ευρωπαϊκό Κοινοβούλιο έχει, επίσης, δικαίωμα ελέγχου επί των

---

[441] Απόφαση ΔΕΕ C-311/18, Maximillian Schrems, της 16ης Ιουλίου 2020. Διαθέσιμο στο https://curia.europa.eu/juris/document/document.jsf;jsessionid=699F5010F9ED77A76EF28523A1A60EE9?text=&docid=228677&pageIndex=0&doclang=EL&mode=req&dir=&occ=first&part=1&cid=10320201.

[442] Απόφαση (ΕΕ) 2016/1250 της Ευρωπαϊκής Επιτροπής, της 12ης Ιουλίου 2016, βάσει της οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την επάρκεια της προστασίας που παρέχεται από την ασπίδα προστασίας της ιδιωτικής ζωής ΕΕ–ΗΠΑ.

[443] Τόσο οι αρχές ασφαλούς λιμένα όσο και η ασπίδα προστασίας για την ιδιωτική ζωή αποτέλεσαν δέσμη κανόνων μεταξύ ΕΕ-ΗΠΑ για τις διατλαντικές ροές δεδομένων.

[444] Ευρωπαϊκή Επιτροπή Ερωτήσεις & Απαντήσεις: Πλαίσιο προστασίας δεδομένων ΕΕ-ΗΠΑ, της 7ης Οκτωβρίου 2022. Διαθέσιμο στο https://www.dpa.gr/sites/default/files/2022-11/E%cf%81%cf%89%cf%84%ce%ae%cf%83%ce%b5%ce%b9%cf%82_%ce%91%cf%80%ce%b1%ce%bd%cf%84%ce%ae%cf%83%ce%b5%ce%b9%cf%82_%ce%a0%ce%bb%ce%b1%ce%af%cf%83%ce%b9%ce%bf%20%ce%a0%cf%81%ce%bf%cf%83%cf%84%ce%b1%cf%83%ce%af%ce%b1%cf%82%20%ce%94%ce%b5%ce%b4%ce%bf%ce%bc%ce%ad%ce%bd%cf%89%ce%bd%20%ce%95%ce%95-%ce%97%ce%a0%ce%91.pdf.

[445] Αυτή περιλαμβάνει, μεταξύ άλλων, δεσμευτικές εγγυήσεις για τον περιορισμό της πρόσβασης στα προσωπικά δεδομένα Ευρωπαίων πολιτών από τις αρχές πληροφοριών των ΗΠΑ στο απολύτως αναγκαίο μέτρο για την περιφρούρηση της εθνικής ασφάλειας, αλλά και την εγκαθίδρυση ενός ανεξάρτητου μηχανισμού προσφυγής, αποτελούμενο από ένα πρωτοβάθμιο όργανο, τον «Υπεύθυνο Προστασίας Ατομικών Δικαιωμάτων» ("Civil Liberties Protection Officer/CLPO") και ένα δευτεροβάθμιο όργανο, το «Αναθεωρητικό Δικαστήριο για την Προστασία των Δεδομένων» ("Data Protection Review Court/DPRC").

[446] Ό.π.

αποφάσεων επάρκειας της Επιτροπής. Ακολούθως, η Ευρωπαϊκή Επιτροπή θα εκδώσει την οριστική απόφαση επάρκειας και από τότε και στο εξής, η διαβίβαση δεδομένων από την ΕΕ θα συντελείται με ασφάλεια στις αμερικανικές εταιρείες που θα έχουν πιστοποιηθεί από το Υπουργείο Εμπορίου των ΗΠΑ.

Η ανάγκη για διαλειτουργικότητα εντός των εικονικών πλατφορμών και κατά μήκος αυτών, καθώς και το δαιδαλώδες, παγκόσμιο δίκτυο συμμετεχόντων που θα δραστηριοποιείται στον εικονικό κόσμο, θα αυξήσει κατακόρυφα τις ροές δεδομένων εκτός ΕΕ και ιδίως τις διαβιβάσεις προς τις ΗΠΑ. Ο Baily Martin ισχυρίζεται ότι το Metaverse πρέπει να αποτελέσει εξαίρεση στους κανόνες μεταφοράς δεδομένων που θεσπίζει ο ΓΚΠΔ για τη διευκόλυνση της λειτουργικότητας και της διαλειτουργικότητάς του[447]. Ωστόσο, αν οι εν λόγω διαβιβάσεις δεν πληρούν ορισμένα αυστηρά κριτήρια προστασίας, τότε τα προσωπικά δεδομένα των χρηστών θα ταξιδεύουν χωρίς εχέγγυα ασφαλείας προς τρίτες χώρες και διεθνείς οργανισμούς, με κίνδυνο πρωτοφανών καταστρατηγήσεων θεμελιωδών ανθρωπίνων δικαιωμάτων και ελευθεριών. Τα κριτήρια που θεσπίζει ο ΓΚΠΔ θα πρέπει, λοιπόν, να διευκρινιστούν από τις αρμόδιες αρχές αναφορικά με την εφαρμογή τους στο Metaverse, και να εξελιχθούν δεόντως, ώστε να ενσωματώνουν απαιτήσεις ασφαλείας βασιζόμενες στα πιο προηγμένα διαθέσιμα κρυπτογραφικά εργαλεία[448].

3.6. Ασφάλεια προσωπικών δεδομένων

Το Metaverse θα μαστίζεται από συνεχείς κυβερνοεπιθέσεις (cyberattacks) και άλλες απειλές, που θα υπονομεύουν την ασφάλεια του εικονικού κόσμου (cybersecurity), ήτοι την ασφάλεια του υλισμικού, λογισμικού, των δικτύων και πληροφοριών που τον απαρτίζουν και τελικά την ασφάλεια των προσωπικών δεδομένων των χρηστών του[449].

Οι απειλές αυτές θα ενταθούν ουσιωδώς, τόσο ποιοτικά όσο και ποσοτικά, λόγω της εγγενούς εξάρτησης του εικονικού περιβάλλοντος από την εκτεταμένη και αδιάλειπτη

---

[447] Ό.π., Martin, B. (2022), σ. 258.

[448] Ό.π., Aamir, O. (2022), σ. 27.

[449] Όπως προκύπτει από την ενωσιακή νομοθεσία (βλ. αιτιολογική σκέψη 49 ΓΚΠΔ) και το διεθνές πρότυπο ISO/IEC 27001 για τη διαχείριση της ασφάλειας των πληροφοριών, ο όρος «ασφάλεια» συνοψίζει τρία βασικά στοιχεία: την εμπιστευτικότητα (Confidentiality), ακεραιότητα (Integrity) [γνησιότητα (Authenticity)] και διαθεσιμότητα (Availability)[449] των (συστημάτων και) πληροφοριών, με άλλα λόγια την εγγύηση ότι οι πληροφορίες είναι προσβάσιμες μόνο από εξουσιοδοτημένους χρήστες, ότι είναι γνήσιες, ακέραιες και ακριβείς και ότι οι χρήστες έχουν ελεύθερη πρόσβαση σε αυτές όταν τις χρειάζονται.

επεξεργασία ευαίσθητων και μη πληροφοριών, της ευρείας ενσωμάτωσης σε αυτό αλγοριθμικών συστημάτων και της ρεαλιστικής 3D απεικόνισης από αυτό του πραγματικού κόσμου, που θα έρθουν να προστεθούν στα ούτως ή άλλως αδιαφιλονίκητα προνόμια του Κυβερνοχώρου υπέρ της εγκληματικότητας και της παρανομίας.

Πιο συγκεκριμένα, φαινόμενα πειρατείας (hacking) και εγκατάστασης κακόβουλου λογισμικού (malware) (πχ. ransomware[450], ιών κ.ά.) αναμένεται ότι θα πλήττουν ειδικές συσκευές εμβύθισης στο Metaverse[451], διασυνδεδεμένους υπολογιστές, λογισμικά και δίκτυα, θέτοντας σε κίνδυνο την ασφάλεια (i.e., εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα) των προσωπικών δεδομένων των χρηστών του. Επιτιθέμενοι στις διατάξεις κεφαλής XR, οι χάκερ θα μπορούν να παρατηρήσουν βιομετρικά και ανθρωπομετρικά στοιχεία του χρήστη (πχ. φωνή, ύψος, μήκος άκρων, κυρίαρχο χέρι, οπτική οξύτητα, φυσική κατάσταση, χρόνος αντίδρασης κ.ά.), τη φυσική τοποθεσία και τον περιβάλλοντα χώρο του (πχ. μέγεθος δωματίου, προσωπικά αντικείμενα κ.ά.), τα χαρακτηριστικά της συσκευής εμβύθισης, του υπολογιστή και του δικτύου (πχ. την ακριβή μάρκα και το μοντέλο της συσκευής XR ή την παλαιότητα και τη μέση τιμή του υπολογιστή κ.ά.), αλλά και τη συμπεριφορά του χρήστη, πληροφορίες από τις οποίες θα είναι σε θέση να συνάγουν και να αξιοποιήσουν υπέρ τους πλήθος απλών και ευαίσθητων δεδομένων για το θύμα (πχ. φύλο, ηλικία, εθνικότητα, οικονομική κατάσταση, υγεία κ.ά.)[452]. Ομοίως, αν καταφέρνουν να δουν ακριβώς τι βλέπει ή ακούει ο χρήστης, θα μπορούν να υποκλέψουν πολύτιμα δεδομένα[453], παρατηρώντας π.χ. την κίνηση των δαχτύλων του όταν εισάγει κωδικούς πρόσβασης στο εικονικό πληκτρολόγιο[454]. Γενικώς, η διαρροή δεδομένων (privacy leakage) στο Metaverse θα είναι δυνατή σε κάθε στάδιο της επεξεργασίας, από τη συλλογή αυτών έως τη διαβίβαση, την εν στενή εννοία επεξεργασία, την αποθήκευσή τους σε συσκευές edge και διακομιστές cloud κ.ο.κ[455].

Επιπλέον, τεχνικές κοινωνικής μηχανικής (social engineering)[456], ιδίως ηλεκτρονικού «ψαρέματος» (phishing)[457], που στοχεύουν ευθέως τους ίδιους τους χρήστες, θα ενισχυθούν

---

[450] Με αυτό το κακόβουλο λογισμικό, οι θύτες κρυπτογραφούν δεδομένα των χρηστών και ζητούν λύτρα για την αποκρυπτογράφησή τους.

[451] Ό.π., Κοντογεώργου, Π., Συρμακέζη, Ζ., Ζούλοβιτς, Μ. (2022), σ. 54.

[452] Ό.π., Nair, V., Garrido, G.M. and Song, D. (2022), σ. 3 επ.

[453] Ό.π., Chen, Z. et al. (2022), σ. 5.

[454] Wang, Y. et al. (2022), σ. 234.

[455] Ό.π.

[456] Ό.π., Di Pietro, R. and Cresci, S. (2021), σ. 284.

σημαντικά εντός του εικονικού κόσμου. Αλγόριθμοι μηχανικής μάθησης είναι πιθανόν να αντιγράφουν τη φωνή, την εμφάνιση και τη συμπεριφορά των άβαταρ της οικογένειας ή των φίλων του χρήστη, με σκοπό να του αποσπάσουν διαπιστευτήρια ή άλλες ευαίσθητες πληροφορίες[458], ενώ έχει ήδη προβλεφθεί ότι οι εξελίξεις στην Τεχνητή Νοημοσύνη θα επιτρέψουν τη δημιουργία αυτοματοποιημένων λογαριασμών που δεν θα ξεχωρίζουν καθόλου από τους ανθρώπους[459]. Η κατασκοπεία (spying) και η παρακολούθηση (stalking) είναι, επίσης, πρακτικές που πιστεύεται ότι θα απειλήσουν σοβαρά την ιδιωτικότητα των χρηστών στο Metaverse[460]. Άβαταρ χρηστών μεταμφιεσμένα σε αντικείμενα θα έχουν τη δυνατότητα να ακολουθούν και παρακολουθούν το χρήστη[461] σε κάθε βήμα, συνάντηση, επίσκεψη ή επιλογή του, το ίδιο και άβαταρ Τεχνητής Νοημοσύνης ή άβαταρ χρηστών που απροκάλυπτα προσπαθούν να αποκτήσουν πρόσβαση στα προσωπικά δεδομένα του για ίδιους σκοπούς.

Όλα τα παραπάνω θα έχουν τρομακτικές συνέπειες στη ζωή των υποκειμένων και θα τα εκθέτουν συνεχώς στον κίνδυνο υλικής και ηθικής βλάβης εντός κι εκτός Metaverse. Κωδικοί πρόσβασης προσωπικών και τραπεζικών λογαριασμών, στοιχεία χρεωστικών και πιστωτικών καρτών, αριθμοί αστυνομικής ταυτότητας και κοινωνικής ασφάλισης, δεδομένα υγείας, ακόμη και συνομιλίες, φωτογραφίες ή βίντεο σεξουαλικού περιεχομένου είναι μεταξύ των βασικών δεδομένων που θα στοχοποιούνται στο εικονικό περιβάλλον. Το φαινόμενο "doxing", δηλαδή η έρευνα και απειλή δημοσιοποίησης προσωπικών δεδομένων τρίτων προσώπων για κακόβουλους σκοπούς (πχ. για τον εκβιασμό ή την παρενόχληση κάποιου), θα οξυνθεί ιδιαίτερα[462], ενώ το ίδιο θα συμβεί και με φαινόμενα διαδικτυακού εκφοβισμού (cyberbullying) ευάλωτων ομάδων (πχ. ανηλίκων, γυναικών κ.ά.). Η κλοπή (εικονικής) ταυτότητας (identity theft), η απομίμηση άβαταρ (avatar duplication)[463], η δημιουργία συνθετικών ταυτοτήτων (synthetic identities) και τα deepfake βίντεο[464], θα χρησιμοποιηθούν ευρέως για την υπόδυση χαρακτήρων, την απόκτηση ωφελημάτων και τη

---

[457] Ό.π., European Parliamentary Research Service (EPRS) (2022), σ. 8.

[458] Huang, Y., Li, Y.J. and Cai, Z. (2023) 'Security and Privacy in Metaverse: A Comprehensive Survey', *Big Data Mining and Analytics*, 6(2), σ. 234–247. Διαθέσιμο στο: https://doi:10.26599/bdma.2022.9020047 Survey, σ. 242.

[459] Ό.π., Di Pietro, R. and Cresci, S. (2021), σ. 286.

[460] Ό.π.

[461] Ό.π., Sandeepa, C., Wang, S. and Liyanage M. (2023), σ. 3.

[462] Ό.π., Kalpokas, I. and Kalpokienė, J. (2023), σ. 100.

[463] Ό.π., European Parliamentary Research Service (EPRS) (2022), σ. 9.

[464] Ό.π., Aamir, O. (2022), σ. 18.

διάπραξη εγκλημάτων ή παράνομων πράξεων. Έτσι, πχ., το Metaverse θα ενισχύσει και δημιουργήσει νέες μεθόδους εκδικητικής πορνογραφίας (revenge porn), καθιστώντας δυνατή τη δημιουργία εικονικών sexbots που θα θυμίζουν κάποιο άλλο φυσικό πρόσωπο[465].

Σύμφωνα με την αρχή της ασφάλειας που θεσπίζει ο ΓΚΠΔ (άρθρο 5 παρ. 1 στοιχ. στ'), τα προσωπικά δεδομένα των υποκειμένων *«υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλεια των δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων»*, ενώ το άρθρο 4 στοιχ. 12 ΓΚΠΔ χαρακτηρίζει ως «παραβίαση δεδομένων προσωπικού χαρακτήρα» την *«παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία»*. Επιπρόσθετα, το άρθρο 32 ΓΚΠΔ επιβάλλει την υποχρέωση τήρησης ενός *«κατάλληλου επιπέδου ασφάλειας»*[466] τόσο στον υπεύθυνο όσο και στον εκτελούντα την επεξεργασία, ενώ εξειδικεύει τα κατάλληλα τεχνικά και οργανωτικά μέτρα που μπορούν αυτοί ενδεικτικά να λαμβάνουν για να εκπληρώσουν δεόντως την ως άνω υποχρέωση (πχ. ψευδωνυμοποίηση ή κρυπτογράφηση προσωπικών δεδομένων, τακτική δοκιμή, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των σχετικών μέτρων για τη διασφάλιση της ασφάλειας κ.ά). Τέλος, το άρθρο 33 ΓΚΠΔ επιβάλλει στους υπευθύνους την υποχρέωση αναγνώρισης, τεκμηρίωσης και αμελλητί γνωστοποίησης των περιστατικών παραβίασης προσωπικών δεδομένων στην αρμόδια εποπτική αρχή, υπό τον όρο ότι ενδέχεται να προκαλέσουν κίνδυνο στα θεμελιώδη δικαιώματα και ελευθερίες των υποκειμένων, ενώ το άρθρο 34 ΓΚΠΔ θεσπίζει την πρόσθετη υποχρέωση ανακοίνωσης των περιστατικών αυτών στα θιγόμενα φυσικά πρόσωπα, εφόσον ο σχετικός κίνδυνος ενδέχεται να είναι υψηλός.

Στο Metaverse αναμένεται να εφαρμοστούν και άλλα νομοθετικά κείμενα για την ασφάλεια, μεταξύ άλλων η Πρόταση Κανονισμού για την ασφάλεια των προϊόντων[467]

---

[465] Ό.π., Kalpokas, I. and Kalpokienė, J. (2023), σ. 105.

[466] *«Λαμβάνοντας υπόψη τις τελευταίες εξελίξεις, το κόστος εφαρμογής και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων».*

[467] Πρόταση Κανονισμού (ΕΕ) του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 30ης Ιουνίου 2021, για τη γενική ασφάλεια των προϊόντων, την τροποποίηση του κανονισμού (ΕΕ) αριθ. 1025/2012

(αφού τεθεί σε εφαρμογή), που έχει στόχο να ενισχύσει το επίπεδο ασφάλειας των προϊόντων που κυκλοφορούν εντός της ενωσιακής αγοράς και η οποία θα ρυθμίζει την ασφάλεια του ειδικού εξοπλισμού εμβύθισης στο Metaverse, η πρόσφατη Οδηγία NIS2[468], με σκοπό την εγκαθίδρυση ενός υψηλού επιπέδου κυβερνοασφάλειας μεταξύ των κρατών-μελών της ΕΕ κ.ο.κ.

Παρατηρούμε ότι ο Ευρωπαίος νομοθέτης έχει απασχοληθεί με το καίριο ζήτημα της ασφάλειας των προσωπικών δεδομένων των υποκειμένων και εν γένει της ασφάλειας στον Κυβερνοχώρο και έχει θωρακίσει πολλαπλώς τα δικαιώματα των πολιτών της ΕΕ, ενσωματώνοντας στην έννομη τάξη κρίσιμα νομοθετικά εργαλεία για τη διασφάλισή της. Ωστόσο, η φύση του Metaverse θα διευκολύνει και, συνεπώς, θα εντείνει όχι μόνο τις κυβερνοεπιθέσεις εναντίον των συστατικών στοιχείων του εικονικού κόσμου, αλλά και γενικότερα τα περιστατικά παραβίασης των προσωπικών δεδομένων των χρηστών του. Στο εικονικό περιβάλλον, όμως, για το οποίο η επεξεργασία προσωπικών δεδομένων θα αποτελεί ακρογωνιαίο λίθο της λειτουργίας του, η αποτυχία ουσιαστικής διαφύλαξης της ασφάλειας αυτών θα σημάνει αυτομάτως και την άμεση εγκατάλειψη και παρακμή του.

Για το λόγο αυτό, υποστηρίζεται ότι ο ΓΚΠΔ θα πρέπει να τροποποιηθεί, ώστε να συμπεριλάβει πρόσθετα ειδικά μέτρα ασφαλείας πέραν της ψευδωνυμοποίησης και της κρυπτογράφησης[469]. Αρκεί, βέβαια, να δοθούν εναρμονισμένες κατευθυντήριες γραμμές από τις αρμόδιες αρχές για το ποιο θεωρείται ως «*κατάλληλο επίπεδο ασφαλείας*» στο Metaverse, με την εξειδίκευση των τεχνικών και οργανωτικών μέτρων που θα πρέπει κατ' ελάχιστον να λαμβάνουν οι συμμετέχοντες για να συμμορφώνονται με τις απαιτήσεις του ΓΚΠΔ. Μεταξύ των προληπτικών και κατασταλτικών μέτρων που θα ήταν σκόπιμο να υιοθετηθούν, συγκαταλέγονται βασικοί μηχανισμοί προστασίας (πχ. τείχη προστασίας-firewalls, προγράμματα προστασίας από ιούς-antivirus, επαλήθευση ταυτότητας-authentication, έλεγχος πρόσβασης-access controls κ.ά.), αλλά και ειδικές τεχνικές πρόληψης και ανίχνευσης διαρροής δεδομένων ("*data leak prevention and detection*

του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και την κατάργηση της οδηγίας 87/357/ΕΟΚ του Συμβουλίου και της οδηγίας 2001/95/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου.

[468] Οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, την τροποποίηση του κανονισμού (ΕΕ) αριθ. 910/2014 και της οδηγίας (ΕΕ) 2018/1972, και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148 (οδηγία NIS 2).

[469] Ό.π., Martin, B. (2022), σ. 259-260.

techniques")[470], η κρυπτογράφηση μηδενικής γνώσης (zero-knowledge encryption)[471], η αποθήκευση των εν στενή εννοία βιομετρικών δεδομένων του χρήστη κρυπτογραφημένων μόνο στο σχετικό υλισμικό[472] κ.ά.

Επίσης, προτείνεται οι πάροχοι της πρόσβασης στον εικονικό κόσμο να εξασφαλίζουν ότι οι χρήστες θα έχουν τη δυνατότητα να ανοίγουν μόνο έναν προσωπικό λογαριασμό στην εκάστοτε πλατφόρμα (one user - one account), στον οποίο θα εισέρχονται με εξελιγμένους και ασφαλείς τρόπους επαλήθευσης ταυτότητας (πχ. βιομετρική ταυτοποίηση μέσω ανάλυσης του μοτίβου βάδισης-gait recognition methods[473]), για την αποτελεσματική διαχείριση της κοινότητας χρηστών από τον κάθε πάροχο και την αύξηση του αισθήματος ευθύνης στα υποκείμενα.

Για τον περιορισμό της παρακολούθησης του χρήστη και των προσωπικών δεδομένων του από τρίτους εντός της πλατφόρμας, προτείνεται να υιοθετηθούν τεχνολογικοί μηχανισμοί, όπως η δυνατότητα (α) δημιουργίας κλώνων του άβαταρ για τη θόλωση της δραστηριότητάς του, (β) αναπαραγωγής ιδιωτικών αντιγράφων των δημόσιων χώρων για την αποκλειστική χρήση τους από το άβαταρ ή (γ) προσωρινού αποκλεισμού τρίτων από τους σχετικούς χώρους, (δ) τηλεμεταφοράς, αορατότητας ή άλλων μορφών μεταμφίεσης του άβαταρ[474], (ε) ενεργοποίησης ζωνών ασφαλείας (security bubbles[475], x-foot barriers[476]) για την προστασία του από ανεπιθύμητες επαφές κ.ά.

Σε κάθε περίπτωση, οι χρήστες θα επιβάλλεται να σέβονται τους Όρους Παροχής Υπηρεσιών που θα έχουν αποδεχθεί, ενώ τυχόν παραβίαση αυτών θα μπορεί να οδηγήσει σε αναστολή λειτουργίας του λογαριασμού τους ή οριστικό αποκλεισμό τους από την πλατφόρμα[477]. Μέσω των σχετικών κανόνων, οι πάροχοι θα πρέπει να απαγορεύουν παραβατικές συμπεριφορές, μεταξύ των οποίων όσες προσβάλλουν την ιδιωτικότητα και τα προσωπικά δεδομένα άλλων χρηστών. Το Minecraft και το World of Warcraft, πχ., ήδη

[470] Ό.π., Huang, Y., Li, Y.J. and Cai, Z. (2023), σ. 239.

[471] Ό.π., Chen, Z. et al. (2022), σ. 6.

[472] Ό.π., Huang, Y., Li, Y.J. and Cai, Z. (2023), σ. 239.

[473] Αντίθετα, η βιομετρική ταυτοποίηση μέσω εικόνας προσώπου ή φωνής είναι πιθανόν να παρακαμφθεί, χάρη στις τεχνολογίες σύνθεσης εικόνας/βίντεο και φωνής (βλ. ό.π., Chen, Z. et al. (2022), σ. 5 - 6).

[474] Ό.π., Di Pietro, R. and Cresci, S. (2021), σ. 285.

[475] Ό.π., Kalpokas, I. and Kalpokienė, J. (2023), σ. 104.

[476] Όπως έχει ρυθμίσει η Meta Platforms (βλ. Mangada Real de Asúa, E. et al. (2022), σ. 23).

[477] Ό.π., Kalpokas, I. and Kalpokienė, J. (2023), σ. 105.

απαγορεύουν το hacking και το διαμοιρασμό προσωπικών δεδομένων τρίτων[478]. Οι πλατφόρμες θα πρέπει να επιτηρούν αποτελεσματικά την εφαρμογή των Όρων τους, μέσω μηχανισμών αναφοράς από τους χρήστες, αυτόματων συστημάτων επισήμανσης ύποπτων χρηστών ή λογαριασμών, ομάδων διαχείρισης εικονικού περιεχομένου, ειδικού λογισμικού τρίτων μερών [479]κ.ο.κ.

Τέλος, η εκπαίδευση των χρηστών είναι εξίσου σπουδαίο εργαλείο αποφυγής και διαχείρισης περιστατικών παραβίασης. Είναι πολύ σημαντικό για αυτούς να είναι σε επαγρύπνηση, να μάθουν να προστατεύουν την εικονική ταυτότητα, τα προσωπικά δεδομένα και τα περιουσιακά στοιχεία τους και να λαμβάνουν για το σκοπό αυτό προληπτικά μέτρα, όπως να μην αποκαλύπτουν υπερβολικά ευαίσθητες προσωπικές πληροφορίες, να ενημερώνουν τις εκδόσεις του εκάστοτε λογισμικού για να καλύπτουν τυχόν κενά ασφαλείας, να χρησιμοποιούν αξιόπιστα antivirus, να ενημερώνονται για τις αναθεωρημένες πολιτικές απορρήτου κ.ά[480].

3.7. Η (ασύμβατη;) σχέση μεταξύ ΓΚΠΔ και Blockchain

Δυνάμει όσων εκτέθηκαν νωρίτερα στην παρούσα (βλ. ενότητα 2.3), στο Blockchain αναμένεται να στηριχθεί μέρος ή το σύνολο των οικονομικών και εμπορικών συναλλαγών που θα εκτελούνται στις υβριδικές πλατφόρμες του Metaverse.

Τα τελευταία χρόνια, η ακαδημαϊκή συζήτηση γύρω από τις νομικές προκλήσεις της τεχνολογίας του Blockchain έχει φέρει στο φως την - εκ πρώτης όψεως - ασυμβατότητα των εγγενών χαρακτηριστικών της με τις γενικές αρχές και το γενικό νομοθετικό καθεστώς προστασίας δεδομένων προσωπικού χαρακτήρα της ΕΕ, τον ΓΚΠΔ. Ενόψει τούτου, αξίζει να αναφερθούμε συνοπτικά στην προβληματική αυτή σχέση, που αναγκαίως θα επηρεάσει την προστασία των προσωπικών δεδομένων των χρηστών στο Metaverse.

Η μελέτη που δημοσίευσε το Ευρωπαϊκό Κοινοβούλιο με τίτλο "Blockchain and the General Data Protection Regulation - Can distributed ledgers be squared with European data protection law?"[481] το 2019, υπογραμμίζει ότι το Blockchain αποτελεί κατ' ουσίαν μία ευρύτερη κατηγορία τεχνολογιών ("*class of technologies*") και κατ' επέκταση, ο έλεγχος της

[478] Ό.π., Kalyvaki, M. (2023), σ. 90.

[479] Ό.π. για τους παρόχους VR.

[480] Ό.π., Chen, Z. et al. (2022), σ. 6.

[481] Ό.π., Panel for the Future of Science and Technology (STOA).

συμβατότητάς του με τον ΓΚΠΔ πρέπει να διενεργείται μόνο κατά περίπτωση[482]. Στο πλαίσιο αυτό, θεωρείται ότι τα ιδιωτικά και περιορισμένης πρόσβασης (permissioned) blockchains[483] είναι πιο εύκολο να σχεδιαστούν με τρόπο συμβατό προς τον ΓΚΠΔ, σε σχέση με τα δημόσια και ελεύθερης πρόσβασης (permissionless).[484]

Τα βασικά σημεία ρήξης μεταξύ του Blockchain και του ΓΚΠΔ είναι τα εξής. Ο ΓΚΠΔ διαπνέεται από την αρχή της λογοδοσίας, σύμφωνα με την οποία ένα συγκεκριμένο και γνωστό στα υποκείμενα και τις εποπτικές αρχές πρόσωπο, ο υπεύθυνος επεξεργασίας, ευθύνεται και λογοδοτεί για την ορθή και καθολική εφαρμογή του. Απεναντίας, το δίκτυο του Blockchain συντηρείται με αποκεντρωμένο τρόπο, μεταξύ απεριόριστου αριθμού αγνώστων χρηστών, καθιστώντας την πρακτική εφαρμογή της αρχής της λογοδοσίας ιδιαίτερα δυσχερή[485]. Επιπλέον, ο ΓΚΠΔ χορηγεί στα υποκείμενα το δικαίωμα διόρθωσης (άρθρο 16) και το δικαίωμα διαγραφής ή αλλιώς το δικαίωμα στη λήθη (άρθρο 17) των προσωπικών δεδομένων τους. Από την άλλη, η τεχνολογία του Blockchain στηρίζεται σε μηχανισμούς συναίνεσης που εξασφαλίζουν τη μόνιμη και αναλλοίωτη διατήρηση των δεδομένων, καθιστώντας τη διαγραφή ή τροποποίησή τους εξαιρετικά επαχθή και χρονοβόρα διαδικασία[486], γεγονός που κατά τ' άλλα ενισχύει την εμπιστοσύνη μεταξύ των απανταχού χρηστών και την ασφάλεια των δεδομένων. Περαιτέρω, ο ΓΚΠΔ θεσπίζει τις αρχές της ελαχιστοποίησης των δεδομένων και του περιορισμού του σκοπού επεξεργασίας. Αντίθετα, το Blockchain επιτρέπει την αέναη προσθήκη δεδομένων στην αλυσίδα *("append-only database")* και την αναπαραγωγή των δεδομένων αυτών από αόριστο αριθμό χρηστών και συσκευών ανά τον κόσμο, ενώ αμφισβητείται αν η, μετά τη διενεργούμενη για τη

---

[482] Ό.π., σ. 3.

[483] Πχ. Hyperledger, Ripple κ.ά. Τρέχουν σε ιδιωτικά δίκτυα (πχ. σε VPN), επομένως η πρόσβαση και η δυνατότητα συμμετοχής σε αυτά δεν είναι ελεύθερες, αλλά εξαρτώνται από την προγενέστερη έγκριση ενός διαχειριστή, συνήθως μίας εταιρείας ή κοινοπραξίας. Ο εν λόγω διαχειριστής κατά κανόνα γνωρίζει την ταυτότητα των συμμετεχόντων. Τα ανωτέρω blockchains χρησιμοποιούνται κατ' αρχήν για συγκεκριμένους επαγγελματικούς ή εμπορικούς/ επιχειρηματικούς σκοπούς. Βλ. ό.π., σ. 5.

[484] Πχ. Bitcoin, Ethereum κ.ά. Οποιοσδήποτε μπορεί να συμμετέχει ως κόμβος, κατεβάζοντας και τρέχοντας το σχετικό λογισμικό, χωρίς να χρειάζεται να λάβει την προηγούμενη άδεια κάποιας κεντρικής οντότητας. Επιπλέον, οποιοσδήποτε μπορεί να αποκτήσει πρόσβαση σε ολόκληρη την αλυσίδα και να δει τις εγγεγραμμένες επ' αυτής συναλλαγές. Ειδικές μηχανές αναζήτησης, οι blockexplorers, επιτρέπουν την ελεύθερη πρόσβαση στα σχετικά δεδομένα. Τα ανωτέρω blockchains αποτελούν δίκτυα ψευδώνυμων χρηστών και χρησιμοποιούνται για γενικούς σκοπούς (Βλ. ό.π., σ. 5).

[485] Ό.π., σελ. II.

[486] Ό.π.

διεκπεραίωση της αρχικής συναλλαγής, επακόλουθη επεξεργασία των προσωπικών δεδομένων που έχουν εγγραφεί στην αλυσίδα, εμπίπτει στον αρχικό σκοπό για τον οποίο αυτά δόθηκαν[487]. Τέλος, εκτιμάται ότι οι εντάσεις μεταξύ της τεχνολογίας του Blockchain και του ΓΚΠΔ οξύνονται από τις ερμηνευτικές ασάφειες που επικρατούν σχετικά με αρκετές διατάξεις του.

Βέβαια, λέγεται και ότι το Blockchain μπορεί να αποτελέσει κατάλληλο εργαλείο για την επίτευξη ορισμένων θεμελιωδών στόχων του ΓΚΠΔ[488]. Ενδεικτικά, διευκολύνει την άσκηση του δικαιώματος στην πρόσβαση των δεδομένων (άρθρο 15 ΓΚΠΔ) και στη φορητότητα αυτών (άρθρο 20 ΓΚΠΔ), ενώ προσφέρει διαφάνεια σε σχέση με το ποιος αποκτά πρόσβαση στα δεδομένα[489], χορηγώντας στα υποκείμενα ουσιαστικό έλεγχο επ' αυτών.

Το πόρισμα της ανωτέρω μελέτης του Ευρωπαϊκού Κοινοβουλίου σε σχέση με τη συμβατότητα του Blockchain και του ΓΚΠΔ καταλήγει στο συμπέρασμα ότι δεν είναι μάλλον αναγκαία η μεταρρύθμιση του τελευταίου για τη συμμόρφωση του πρώτου. Αντιθέτως, προτείνεται να δοθεί συντονισμένη ρυθμιστική καθοδήγηση από τις εθνικές εποπτικές αρχές για το θέμα υπό τις οδηγίες του ΕΣΠΔ, αλλά και να αναθεωρηθούν ορισμένες κατευθυντήριες γραμμές της Ομάδας προστασίας δεδομένων του άρθρου 29 που ενισχύουν την ανασφάλεια δικαίου σε σχέση με συγκεκριμένες έννοιες του ΓΚΠΔ, όπως η Γνώμη 05/2014 για τις τεχνικές ανωνυμοποίησης[490] [491]. Παράλληλα, προωθείται η θέσπιση κωδίκων δεοντολογίας (άρθρο 40 ΓΚΠΔ) και μηχανισμών πιστοποίησης (άρθρο 42 ΓΚΠΔ) για την by design εφαρμογή των γενικών αρχών της ευρωπαϊκής νομοθεσίας για την προστασία δεδομένων στο ειδικότερο πλαίσιο επεξεργασίας δεδομένων μέσω του Blockchain και την ευχερέστερη απόδειξη της συμμόρφωσης από τους συμμετέχοντες[492]. Τέλος, η σχετική μελέτη υπογραμμίζει τη σπουδαιότητα χρηματοδότησης διεπιστημονικής έρευνας, ώστε να δοθούν πρακτικές λύσεις σε τεχνικής και οργανωτικής φύσεως ζητήματα

---

[487] Ό.π.

[488] Ό.π., Panel for the Future of Science and Technology (STOA) (2019), σ. III.

[489] Ό.π.

[490] Ομάδα προστασίας δεδομένων του άρθρου 29, Γνώμη 05/2014 σχετικά με τις τεχνικές ανωνυμοποίησης, της 10ης Απριλίου 2014. Διαθέσιμο στο: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_el.pdf.

[491] Ό.π., Panel for the Future of Science and Technology (STOA) (2019), σ. IV.

[492] Ό.π., Panel for the Future of Science and Technology (STOA) (2019), σ. IV-V.

που μοιάζουν ασύμβατα προς τον ΓΚΠΔ, όπως ο καθορισμός των τεχνικών μεθόδων για τη συμμόρφωση προς το άρθρο 17[493].

Συμπερασματικά, με την τήρηση των προτάσεων του Ευρωπαϊκού Κοινοβουλίου, οι πάροχοι υπηρεσιών Metaverse θα μπορούν να συμμορφώνονται στις απαιτήσεις του ΓΚΠΔ, αναφορικά με τη διενεργούμενη επεξεργασία των προσωπικών δεδομένων των χρηστών που θα αποθηκεύονται στα blockchains που θα χρησιμοποιούν στις υβριδικές πλατφόρμες τους για την εκτέλεση οικονομικών ή/και εμπορικών συναλλαγών.

ΙΙΙ. ΣΥΜΠΕΡΑΣΜΑΤΑ

Η αποίκηση της ανθρωπότητας σε άλλον πλανήτη εκτιμάται ότι τελικά θα συμβεί πολύ νωρίτερα από το προσδοκώμενο· μόνο που ο πλανήτης αυτός δεν είναι ο Άρης ούτε ανήκει στο ηλιακό μας σύστημα, είναι το Metaverse και προς το παρόν δεν υπάρχει.

Ούτε θα υπάρξει όμως ποτέ στον υλικό κόσμο. Ορθότερα ιδωμένο ως η μελλοντική μορφή του Διαδικτύου, το Metaverse φιλοδοξεί να μετασχηματίσει το κοινωνικοοικονομικό μοντέλο του 21ου αιώνα, προσφέροντας στον άνθρωπο την ευκαιρία να ζήσει εικονικά μια παράλληλη, απόλυτα ρεαλιστική και ολοκληρωμένη συναλλακτική καθημερινότητα, υπό μορφή ενός τρισδιάστατου ψηφιακού εαυτού, γνωστού ως «άβαταρ».

Οι επιμέρους τεχνολογίες που θα επιτρέψουν την εμβύθισή μας στο Metaverse είναι μεν ήδη γνωστές, ωστόσο πρέπει να βελτιωθούν και ενδεχομένως να συμπληρωθούν από νέα τεχνολογικά εργαλεία, για την επιτυχή υλοποίησή του. Πρωταγωνιστικό ρόλο θα κατέχει, ασφαλώς, η Εκτεταμένη Πραγματικότητα, η Τεχνητή Νοημοσύνη, το Διαδίκτυο των Πραγμάτων, το Υπολογιστικό Νέφος, τα ασύρματα δίκτυα 5ης γενιάς και το Blockchain. Οι τεχνολογίες αυτές θα είναι απαραίτητες για την ευρεία, μαζική, αδιάλειπτη και αποτελεσματική επεξεργασία πληροφοριών και δη των προσωπικών δεδομένων των χρηστών του Metaverse, η οποία θα αποτελέσει ακρογωνιαίο λίθο και εκ των ων ουκ άνευ συνθήκη για τη λειτουργία του.

Κανείς δεν γνωρίζει ούτε είναι δυνατόν να προβλέψει ποιο θα είναι το πραγματικό αντίκτυπο του Metaverse στη ζωή μας. Σε μια ουτοπική εκδοχή του, υποστηρίζεται ότι θα ενισχύσει και επαναπροσδιορίσει τον τομέα των εμπορικών και οικονομικών συναλλαγών, τις τέχνες και την ψυχαγωγία, την εργασία, την εκπαίδευση, την ιατρική και την υγεία, τις έξυπνες πόλεις, τον τουρισμό κ.ά. Το βέβαιο, όμως, είναι ότι παρουσιάζει αναρίθμητες

[493] Ό.π., Panel for the Future of Science and Technology (STOA) (2019), σ. V.

ευκαιρίες για οικονομική άνθιση κι εν γένει συγκέντρωση εξουσίας όσων θα παρέχουν την πρόσβαση σε αυτό και όσων θα συμμετέχουν για επιχειρηματικούς, επαγγελματικούς, πολιτικούς ή άλλους μη καθαρά ιδιωτικούς σκοπούς. Γι' αυτό και έχουν σπεύσει να επενδύσουν στο Metaverse, με τον έναν ή τον άλλον τρόπο, τεχνολογικοί κολοσσοί, εμπορικά σήματα, αποκεντρωμένες κοινότητες και κρατικοί σχηματισμοί από όλο τον κόσμο, οδηγώντας στην ανάπτυξη ανταγωνιστικών οραμάτων για τη μορφή του, κυρίως για το ποιος θα κυβερνά επί της ουσίας όχι το ίδιο, αλλά τις εικονικές πλατφόρμες που θα το απαρτίζουν.

Αν και είναι πιθανό να συνυπάρξουν τόσο ιδιωτικές-συγκεντρωτικές-κλειστές-WEB 2.0, όσο και κοινόχρηστες-αποκεντρωμένες-ανοιχτές-WEB 3.0 Metaverse πλατφόρμες στη σχετική αγορά, η γνώμη που προβάλλεται στην παρούσα διπλωματική εργασία είναι ότι τελικά, μάλλον θα επικρατήσουν υβριδικές μορφές, την εικονική υποδομή των οποίων θα προσφέρουν ιδιωτικές εταιρείες, ενσωματώνοντας παράλληλα αποκεντρωμένα εργαλεία δήθεν για τη δημοκρατικοποίηση του εικονικού κόσμου.

Στο πλαίσιο αυτό, η ρύθμιση του Metaverse είναι αναγκαία για την προστασία της ιδιωτικότητας των χρηστών του και την αποφυγή της μονοπώλησής του από ισχυρούς ιδιωτικούς παράγοντες, που έχουν κακόφημο παρελθόν για τις υιοθετούμενες μεθόδους επεξεργασίας προσωπικών δεδομένων. Η ΕΕ οφείλει να αξιολογήσει την προσφορότητα του ΓΚΠΔ να εφαρμοστεί στο Metaverse, ως γενικού νομοθετικού πλαισίου προστασίας προσωπικών δεδομένων που ρυθμίζει, μεταξύ άλλων, τον ψηφιακό χώρο. Πράγματι, χωρίς αποτελεσματικά νομοθετικά και ρυθμιστικά εργαλεία, ο εικονικός κόσμος θα λειτουργήσει ως ναρκοπέδιο για τα υποκείμενα, τα προσωπικά δεδομένα των οποίων θα αξιοποιούνται εκτενώς και εν αγνοία τους από απροσδιόριστο αριθμό τρίτων μερών, με αμφίβολης ηθικής και νομιμότητας ιδιωτικά συμφέροντα.

Ο ΓΚΠΔ θεσπίστηκε μεν πρόσφατα, εντούτοις σε μια εποχή που το Metaverse ανήκε αποκλειστικά στη σφαίρα της επιστημονικής φαντασίας. Ο Ευρωπαίος νομοθέτης δεν θα μπορούσε να το έχει λάβει υπόψη του, ως έναν κόσμο που πράγματι θα ερχόταν στο φως. Σε καμία περίπτωση, λοιπόν, δεν μπορεί να κριθεί ασφαλές και ικανοποιητικό το επίπεδο προστασίας της ενωσιακής νομοθεσίας προσωπικών δεδομένων ενόψει της έλευσης του Metaverse. Αυτό μοιάζει *φύσει ασύμβατο* με τις γενικές αρχές ελαχιστοποίησης των δεδομένων και περιορισμού της χρονικής περιόδου αποθήκευσης και του σκοπού επεξεργασίας τους που θεσπίζει ο ΓΚΠΔ. Ταυτόχρονα, θα εντείνει τις ήδη υπάρχουσες και

επιπλέον, θα εγείρει καινοφανείς *νομικές προκλήσεις*, σε σχέση με τις γενικές αρχές της λογοδοσίας, διαφάνειας, νομιμότητας και ασφάλειας της επεξεργασίας και την άσκηση των δικαιωμάτων των υποκειμένων, ενώ η χρήση τεχνολογιών Blockchain για τη διεκπεραίωση οικονομικών και εμπορικών συναλλαγών, θα αναβιώσει τις εντάσεις του τελευταίου με τον ΓΚΠΔ, ιδίως σε σχέση με το δικαίωμα διαγραφής και διόρθωσης των δεδομένων.

Παρά ταύτα, ο ΓΚΠΔ αποτελεί το πιο ισχυρό νομοθέτημα προστασίας προσωπικών δεδομένων σε παγκόσμιο επίπεδο, εμπνέοντας και άλλους νομοθέτες να ακολουθήσουν το ρυθμιστικό παράδειγμα της ΕΕ (βλ. νόμο "CCPA" Καλιφόρνιας). Ταυτόχρονα, διαπνέεται από τεχνολογική ουδετερότητα, υπό την έννοια ότι δεν αναφέρεται σε συγκεκριμένες τεχνολογικές μεθόδους επεξεργασίας δεδομένων, ενώ η γλώσσα που χρησιμοποιεί είναι ιδιαίτερα γενική και εύπλαστη, ώστε να μπορεί να εφαρμοστεί αποτελεσματικά σε κάθε τεχνολογία. Άλλωστε, το Metaverse θα συντεθεί ως επί το πλείστον από ήδη υπάρχουσες τεχνολογίες, αλλάζοντας ριζικά τον τρόπο με τον οποίο αλληλεπιδρούμε με τα ψηφιακά περιβάλλοντα, με αποτέλεσμα να μην αντιμετωπίζεται κατ' αρχήν αυτό καθ' εαυτό ως μια νέα τεχνολογία. Γι' αυτό το λόγο, παρά την όποια εκ πρώτης όψεως ασυμβατότητα και εγγενή δυσκολία εφαρμογής του στο εικονικό περιβάλλον, ο ΓΚΠΔ πρέπει -και δύναται- να αποτελέσει τη βάση για την προστασία των προσωπικών δεδομένων των χρηστών του Metaverse. Το τελευταίο δεν πρέπει να αποκλείσει την εφαρμογή του ΓΚΠΔ στον εικονικό κόσμο, και αντίστοιχα, ο ΓΚΠΔ δεν πρέπει να σταθεί εμπόδιο στην επικράτηση του Metaverse στην ψηφιακή αγορά. Ωστόσο, το επίπεδο νομοθετικής προστασίας που επιφυλάσσει σήμερα, *ως έχει*, στα υποκείμενα, *δεν* μπορεί, όπως είδαμε, σε καμία περίπτωση, να κριθεί αρκετό για την προστασία των προσωπικών δεδομένων τους στο Metaverse.

Σε μια δυστοπική εκδοχή του, το Metaverse θα επεξεργάζεται με αδιαφανείς και μη νόμιμες μεθόδους έναν πρωτόγνωρο όγκο και εύρος βιομετρικών και συμπεριφορικών δεδομένων του χρήστη, που θα εξάγονται από τον ειδικό εξοπλισμό εμβύθισης και θα οδηγούν ανά πάσα στιγμή, με τη χρήση προηγμένων αλγοριθμικών εργαλείων, σε πλήρη ταυτοποίησή του, αλλά και σκιαγράφηση του ψυχογραφικού προφίλ του. Τα δεδομένα αυτά, συνδυαστικά με άλλα δεδομένα που ο χρήστης θα εισάγει οικειοθελώς ή θα παρατηρούνται και συνάγονται από την εμφάνιση του άβατάρ του, θα καθιστούν τον τελευταίο απόλυτα διαφανή στο εικονικό περιβάλλον, ενώ η πώληση αυτών σε τρίτες

εταιρείες εκτός Metaverse θα έχει παρόμοια αποτελέσματα και στην πραγματική του ζωή. Ο χρήστης θα στοχεύεται διαρκώς με απόλυτα εξατομικευμένο διαφημιστικό (και όχι μόνο) περιεχόμενο, που θα ενσωματώνεται αθόρυβα στο σκηνικό της εικονικής εμπειρίας, θα αντικατοπτρίζει τις πιο ενδόμυχες ανάγκες και προτιμήσεις του και θα συνδιαμορφώνει νέες, οδηγώντας τον σε απόλυτη οικονομική και πολιτική χειραγώγηση και πλήρη απώλεια της αυτονομίας του. Η ευρύτατη χρήση εργαλείων Τεχνητής Νοημοσύνης θα οξύνει ρατσιστικά φαινόμενα, τόσο μεταξύ της κοινότητας χρηστών, όσο και από αλγοριθμικά συστήματα λήψης αποφάσεων που θα αποφασίζουν ερήμην τους για τις έννομες και ουσιώδεις σχέσεις και καταστάσεις τους, πολλές φορές συνάγοντας για αυτούς εσφαλμένα συμπεράσματα από τα αληθινά ή αναληθή δεδομένα τους. Οι υπεύθυνοι επεξεργασίας θα κρύβονται πίσω από συνεχείς, αλληλεπικαλυπτόμενες, μακροσκελείς και δυσνόητες πολιτικές απορρήτου και θα παραλείπουν νόμιμες υποχρεώσεις τους. Τα υποκείμενα δεν θα γνωρίζουν σε ποιον να απευθυνθούν για να ασκήσουν τα δικαιώματά τους, ενώ θα εγκλωβίζονται εντός μιας εικονικής πλατφόρμας (locked-in), λόγω έλλειψης υιοθέτησης διαλειτουργικών προτύπων από τους παρόχους πρόσβασης στο Metaverse και ουσιαστικής απενεργοποίησης του δικαιώματός τους στη φορητότητα. Βέβαια, η ανάγκη για διαλειτουργικότητα του εικονικού κόσμου θα αυξήσει εκθετικά τις διαβιβάσεις, αλλά και τις ροές δεδομένων εκτός ΕΕ, υπονομεύοντας την ασφάλεια των δεδομένων των χρηστών του. Η χρήση τεχνολογιών Blockchain θα τους αποτρέψει, επίσης, από το να διορθώνουν ή να διαγράφουν τα προσωπικά δεδομένα τους, όπως δικαιούνται δυνάμει του ΓΚΠΔ. Τελικά, η ιδιωτικότητά τους θα παραβιάζεται συστηματικά και όσο ποτέ άλλοτε, τόσο από εσωτερικές απειλές, όσο και από κυβερνοεγκληματίες, που θα σπεύσουν να εκμεταλλευτούν τις αδυναμίες του εικονικού κόσμου, αλλά και την αφέλεια των χρηστών του, για να αποκτήσουν οικονομικά ή άλλα οφέλη εις βάρος τους.

Ο ρόλος της ΕΕ είναι, εν προκειμένω, καθοριστικός και γι' αυτό, πρέπει να λάβει ηγετικές πρωτοβουλίες προς εξισορρόπηση αντίρροπων δικαιωμάτων. Ειδικότερα, οφείλει να *αναθεωρήσει εγκαίρως* τον ΓΚΠΔ για να μπορέσει να ανταποκριθεί ασφαλώς και επαρκώς στις νομικές προκλήσεις που θα οξύνει και αναδείξει το Metaverse σε σχέση με την ιδιωτική ζωή των χρηστών του. Θέση της γράφουσας είναι ότι οι βιομετρικού τύπου πληροφορίες οι οποίες μέχρι σήμερα είναι αδύνατον να συλλεχθούν σωρευτικά και δη στο πλαίσιο της αλληλεπίδρασης του ατόμου με απολύτως ρεαλιστικούς και ολοκληρωμένους εικονικούς κόσμους, πρέπει να υπαχθούν ρητώς και με σαφήνεια στην κατηγορία των

ευαίσθητων, βιομετρικών δεδομένων των άρθρων 9 παρ. 1 και 4 παρ. 14 ΓΚΠΔ, δυνάμει των οποίων η επεξεργασία τους κατ' αρχήν απαγορεύεται. Προτείνεται, επίσης, να θεσπιστεί στο άρθρο 9 ΓΚΠΔ νόμιμη βάση αντίστοιχη αυτής του άρθρου 6 παρ. 1 στοιχ. β' ΓΚΠΔ για τα βιομετρικά δεδομένα σε εικονικά περιβάλλοντα, ώστε, όσα από αυτά ρυθμιστούν ως απολύτως αναγκαία για την ουσιαστική λειτουργία του Metaverse, να υπόκεινται σε νόμιμη επεξεργασία. Η οπτικοποίηση των πολιτικών απορρήτου πρέπει, επίσης, να θεσπιστεί ως υποχρέωση των υπευθύνων επεξεργασίας που δραστηριοποιούνται σε εικονικούς κόσμους, ενώ η κατάρτιση προφίλ που βασίζεται στην παρακολούθηση των βιομετρικών δεδομένων και της συμπεριφοράς των υποκειμένων σε τέτοια περιβάλλοντα, πρέπει όσο το δυνατόν να περιοριστεί.

Οι διατάξεις, πάντως, του ΓΚΠΔ για την υποχρέωση των υπευθύνων περί λήψης κατάλληλων τεχνικών και οργανωτικών μέτρων by design και by default, έκδοσης εκτίμησης αντικτύπου για την υψηλού κινδύνου επεξεργασία, αλλά και τη δυνατότητα συμμετοχής τους σε κώδικες δεοντολογίας και μηχανισμούς πιστοποίησης, αποτελούν σπουδαία νομοθετικά εργαλεία, που θα λειτουργήσουν ως *δικλείδες ασφαλείας* για την προστασία των χρηστών στο Metaverse.

Το ΕΣΠΔ οφείλει να διασφαλίσει τη *σύννομη και συνεκτική ερμηνεία και εφαρμογή του ΓΚΠΔ στο Metaverse* από όλους όσους εμπίπτουν στο εδαφικό πεδίο εφαρμογής του, αναθεωρώντας ή εκδίδοντας νέες κατευθυντήριες γραμμές και συστάσεις και αποσαφηνίζοντας έννοιες που θα χρειαστούν επαναπροσδιορισμό στον εικονικό κόσμο (βλ. εδαφικό πεδίο εφαρμογής, έννοια βιομετρικών δεδομένων, διάκριση υπευθύνων και εκτελούντων, τεχνολογικά μέτρα προστασίας κ.ο.κ.). Αντίστοιχα, οι *εθνικές εποπτικές αρχές* θα πρέπει να συμμορφώνονται προς τις κατευθύνσεις του ΕΣΠΔ και να εκδίδουν εναρμονισμένες κατευθυντήριες γραμμές, γνωμοδοτήσεις, αποφάσεις κ.ά.

Η *αυτορρύθμιση (self-regulation) των οικείων παρόχων* μέσω προστατευτικών της ιδιωτικότητας Όρων Παροχής Υπηρεσιών, αποτελεσματικών μηχανισμών ταυτοποίησης χρήστη, ελέγχου της εισόδου στην πλατφόρμα και του διακινούμενου σε αυτήν περιεχομένου κ.ά., είναι, επίσης, ιδιαίτερα σημαντική για την ουσιαστική προστασία των προσωπικών δεδομένων των χρηστών στο Metaverse. Το ίδιο ουσιώδης, βέβαια, είναι και η *εκπαίδευση των υποκειμένων*, που έχει ήδη αποδειχθεί ότι συνήθως αγνοούν ή ενίοτε αδιαφορούν για τους επικείμενους κινδύνους που εγκυμονεί ο Κυβερνοχώρος για τα

προσωπικά δεδομένα τους και κατ' επέκταση για θεμελιώδη δικαιώματα και ελευθερίες τους.

Σαφώς, τα παραπάνω σημαίνουν και προϋποθέτουν την υλοποίηση αμοιβαίων υποχωρήσεων και από τις δύο πλευρές, τόσο από τον επιχειρηματικό και πολιτικό κόσμο που έχει άμεσο συμφέρον να δραστηριοποιηθεί στο χώρο του Metaverse, όσο και από τα ρυθμιστικά και εποπτικά όργανα της ΕΕ που καλούνται να ρυθμίσουν τον εικονικό αυτό κόσμο προσαρμόζοντας το ήδη υπάρχον νομοθετικό και ρυθμιστικό πλαίσιο. Είναι βέβαιο ότι σε αυτήν την περίπτωση, το Metaverse θα απέχει αρκετά από αυτό που φαντάζονται και φιλοδοξούν σήμερα να δημιουργήσουν οι κατασκευαστές, επενδυτές και άλλοι άμεσα ενδιαφερόμενοι. Ακόμη δε κι αν τελικά κριθεί από την ΕΕ ότι η τροποποίηση του ΓΚΠΔ δεν αποτελεί ικανοποιητική λύση και αποφασίσει η τελευταία να θεσπίσει ειδική νομοθεσία για το Metaverse, μια τέτοια ειδική ρύθμιση δεν θα πρέπει να παραγνωρίζει τις θεμελιώδεις αρχές προστασίας προσωπικών δεδομένων του ΓΚΠΔ, οι οποίες ως γενικό κανονιστικό πλαίσιο θα πρέπει να εξακολουθούν να εφαρμόζονται.

Σε κάθε περίπτωση, οι νομικές προκλήσεις και οι κίνδυνοι που αναλύθηκαν ανωτέρω και που αδιαμφισβήτητα θα απειλήσουν την ιδιωτικότητα των χρηστών στο Metaverse, χρήζουν *διεπιστημονικής προσέγγισης και διαλόγου*, όπου καίριο ρόλο θα κατέχει, πέραν της νομικής, η επιστήμη των υπολογιστών, της μηχανικής, η φιλοσοφία, οι κοινωνικές επιστήμες κ.ο.κ[494].

IV. ΕΠΙΛΟΓΟΣ

Η ιδέα για το Metaverse απηχεί και επιβεβαιώνει τελικά την ανθρώπινη φύση μας. Ο διαρκής αγώνας για εξέλιξη, για σύσφιξη διαπροσωπικών και κοινωνικών δεσμών, αλλά και η συνεχής αμφισβήτηση και επαναπροσδιορισμός των μέσων αυτού του αγώνα, ώθησαν τον άνθρωπο να ονειρευτεί μια δεύτερη εικονική ζωή σε ένα παράλληλο άυλο σύμπαν. Είναι όμως τα οικονομικά, πολιτικά και άλλα ίδια συμφέροντα που του έδωσαν το κίνητρο να επιδιώξει εν τοις πράγμασι αυτό το όραμα.

Οι κίνδυνοι μιας τέτοιας πλήρως εικονικής ή επαυξημένης πραγματικότητας δεν είναι καθόλου «εικονικοί», αλλά είναι οπωσδήποτε «επαυξημένοι» (τόσο στο πεδίο των προσωπικών δεδομένων και εν γένει της ιδιωτικότητας, όσο και σε σχέση με τη διανοητική ιδιοκτησία, το δίκαιο προστασίας καταναλωτή, το εμπράγματο δίκαιο, το φορολογικό

[494] Ό.π., Di Pietro, R. and Cresci, S. (2021), σ. 282.

δίκαιο, το ποινικό δίκαιο, την κυβερνοασφάλεια, το δίκαιο ανταγωνισμού, τη νομοθεσία για τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες κ.ο.κ.).

Γι' αυτό και τυχόν υπορρύθμιση του Metaverse θα αναβιώσει εφιαλτικά σενάρια, μεταξύ άλλων, περί μαζικών παρακολουθήσεων, υποδούλωσης του ανθρώπου στις μηχανές και υπερσυγκέντρωσης οικονομικής και πολιτικής εξουσίας από ιδιωτικές εταιρείες εις βάρος των χρηστών του. Η υπερρύθμισή του ωστόσο θα αποθαρρύνει την εισαγωγή ή άνθισή του στην αφιλόξενη ενωσιακή αγορά, στερώντας από τους Ευρωπαίους πολίτες ένα πολύτιμο τεχνολογικό εργαλείο που υπόσχεται να ανατρέψει τη ζωή τους, επεκτείνοντας τις δυνατότητες και τα όριά της.

Ο λόγος ανήκει τώρα στα θεσμικά και ανεξάρτητα όργανα της ΕΕ για να χαράξουν σε συνεργασία με τον επιχειρηματικό κόσμο, την επιστημονική κοινότητα, αλλά και τους πολίτες της, τη –δύσβατη- πορεία προς έναν συναρπαστικό και ταυτόχρονα ασφαλή εικονικό κόσμο.

V. ΒΙΒΛΙΟΓΡΑΦΙΑ

ΑΡΘΡΟΓΡΑΦΙΑ

Aamir, O. (2022) 'Metaverse and its regulation', *SSRN Electronic Journal*, 29 Δεκεμβρίου. Διαθέσιμο στο: https://doi.org/10.2139/ssrn.4306357

Anidjar, L.Y., Packin, N.G. and Panezi, A. (2023) 'The Matrix of Privacy: Data Infrastructure in the AI-Powered Metaverse', *SSRN Electronic Journal*. 24 Φεβρουαρίου. Διαθέσιμο στο: https://doi.org/10.2139/ssrn.4363208

Bloomberg, S. (2023) 'Political advertising in virtual reality', *SSRN Electronic Journal*. 23 Φεβρουαρίου. Διαθέσιμο στο: https://doi:10.2139/ssrn.4245908

Bolognini, L. and Carpenelli, M. E. (2022) 'The future of personal data in the Metaverse', *Zenodo*. Διαθέσιμο στο: https://doi.org/10.5281/zenodo.6413046

Chen, Z. et al. (2022) 'Metaverse Security and Privacy: An Overview', *2022 IEEE International Conference on Big Data (Big Data)*. Διαθέσιμο στο: https://doi.org/10.1109/bigdata55660.2022.10021112

Di Pietro, R. and Cresci, S. (2021) 'Metaverse: Security and Privacy Issues', *2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications*

(TPS-ISA), Ατλάντα, Τζόρτζια, ΗΠΑ, 13-15 Δεκεμβρίου. IEEE, σ. 281-288. Διαθέσιμο στο: https://doi.org/10.1109/tpsisa52974.2021.00032

Dick, E. (2021) 'Balancing user privacy and innovation in Augmented and Virtual Reality', *Information Technology and Innovation Foundation*, 4 Μαρτίου. Διαθέσιμο στο: https://itif.org/publications/2021/03/04/balancing-user-privacy-and-innovation-augmented-and-virtual-reality/ [Πρόσβαση 14 Μαΐου 2023]

Fernandez, C. B. and Hui, P. (2022) 'Life, the Metaverse and Everything: An Overview of Privacy, Ethics, and Governance in Metaverse', *2022 IEEE 42nd International Conference on Distributed Computing Systems Workshops (ICDCSW)*, Μπολόνια, Ιταλία, 10 Ιουλίου. IEEE, σ. 272-277. Διαθέσιμο στο: https://doi.org/10.1109/icdcsw56584.2022.00058

Floridi, L. (2022) 'Metaverse: a Matter of Experience', *SSRN Electronic Journal*. 13 Ιουνίου. Διαθέσιμο στο: https://doi.org/10.2139/ssrn.4121411

Heller, B. (2020) 'Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psychography, and the Law', *Vanderbilt Journal of Entertainment & Technology Law*, 23(1), σ. 1-51. Διαθέσιμο στο: https://scholarship.law.vanderbilt.edu/cgi/viewcontent.cgi?article=1000&context=jetlaw

Huang, Y., Li, Y.J. and Cai, Z. (2023) 'Security and Privacy in Metaverse: A Comprehensive Survey', *Big Data Mining and Analytics*, 6(2), σ. 234–247. Διαθέσιμο στο: https://doi:10.26599/bdma.2022.9020047

Huynh-The, T. et al. (2023) 'Artificial intelligence for the metaverse: A survey', *Engineering Applications of Artificial Intelligence*, 117, 105581. Διαθέσιμο στο: https://doi.org/10.1016/j.engappai.2022.105581

Kalyvaki, M. (2023) 'Navigating the metaverse business and legal challenges: Intellectual property, privacy, and jurisdiction', *Journal of Metaverse*, 3(1), σ. 87-92. Διαθέσιμο στο: https://doi.org/10.57019/jmv.1238344

Kevins, J. (2022) 'Metaverse as a New Emerging Technology: An Interrogation of Opportunities and Legal Issues: Some Introspection', *SSRN Electronic Journal*. 9 Μαρτίου. Διαθέσιμο στο: https://doi.org/10.2139/ssrn.4050898

Kim, Y. (2022) 'Virtual Reality Data and Its Privacy Regulatory Challenges: A Call to Move Beyond Text-Based Informed Consent', *California Law Review*, 110(2), σ. 225-256. Διαθέσιμο στο: https://doi.org/10.15779/Z380Z70X6P

Kosta, E. et al. (2010) 'Data protection issues pertaining to social networking under EU law', *Transforming Government: People, Process and Policy*, 4(2), σ. 193–201. Διαθέσιμο στο: https://doi.org/10.1108/17506161011047406

Kröger, J.L., Lutz, O. and Müller, F. (2019) 'What Does Your Gaze Reveal About You? On the Privacy Implications of Eye Tracking', *Springer Link.* Διαθέσιμο στο: https://link.springer.com/chapter/10.1007/978-3-030-42504-3_15

Lim, W.M. et al. (2022) 'Realizing the Metaverse with Edge Intelligence: A Match Made in Heaven' *IEEE Wireless Communications*, σ. 1–9. Διαθέσιμο στο: https://doi.org/10.1109/mwc.018.2100716

Madary, M. and Metzinger, T. K. (2016) 'Real Virtuality: A Code of Ethical Conduct. Recommendations for Good Scientific Practice and the Consumers of VR-Technology', *Frontiers in Robotics & AI*, 3 (No 3). Διαθέσιμο στο: https://www.frontiersin.org/articles/10.3389/frobt.2016.00003/full

Mangada Real de Asúa, E. et al. (2022) 'The Metaverse: Challenges and regulatory issues', *SciencesPo. Διαθέσιμο στο: https://www.sciencespo.fr/public/sites/sciencespo.fr.public/files/Metaverse-Group-report-final-draft-June-12-1.pdf*

Martin, B. (2022) 'Privacy in a Programmed Platform: How the General Data Protection Regulation Applies to the Metaverse', *Harvard Journal of Law & Technology*, 36(1), σ. 235-261. Διαθέσιμο στο: https://jolt.law.harvard.edu/assets/articlePDFs/v36/Martin-Privacy-in-a-Programmed-Platform.pdf

Miller, M.R. et al. (2020) 'Personal identifiability of user tracking data during observation of 360-degree VR video', *Scientific Reports*, 10 (No 17404). Διαθέσιμο στο: https://doi.org/10.1038/s41598-020-74486-y

Nair, V., Garrido, G.M. and Song, D. (2022) 'Exploring the Unprecedented Privacy Risks of the Metaverse', *arXiv (Cornell University).* Διαθέσιμο στο: https://doi.org/10.48550/arXiv.2207.13176

Nevelsteen, K.J. (2017) 'Virtual World, Defined from a Technological Perspective, and Applied to Video Games, Mixed Reality and the Metaverse', *Computer Animation and Virtual Worlds*, 29(1). Διαθέσιμο στο: https://doi.org/10.1002/cav.1752

Olivi, G., Anselmi, N. and Miele, C.O. (2020) 'Virtual Reality: Top Data Protection Issues to Consider' *The Journal of Robotics, Artificial Intelligence & Law*, 3(2), σ. 141-145. Διαθέσιμο στο: https://search.informit.org/doi/10.3316/agispt.20230202082765

Rosenberg, L.B. (2022) 'Regulating the Metaverse, a Blueprint for the Future', *Lecture Notes in Computer Science (LNCS)*, 13445, σ. 263–272. Διαθέσιμο στο: https://doi.org/10.1007/978-3-031-15546-8_23

Sandeepa, C., Wang, S. and Liyanage M. (2023) 'Privacy of the Metaverse: Current Issues, AI Attacks, and Possible Solutions', *IEEE International Conference on Metaverse Computing, Networking and Applications (IEEE MetaCom 2023)*, Κιότο, Ιαπωνία, 26-28 Ιουνίου 2023. ResearchGate (προδημοσίευση). Διαθέσιμο στο: https://www.researchgate.net/publication/369331696_Privacy_of_the_Metaverse_Current_Issues_AI_Attacks_and_Possible_Solutions

Sebastian, G. (2023) 'A descriptive study on Metaverse', *International Journal of Security and Privacy in Pervasive Computing*, 15(1), σ. 1–14. Διαθέσιμο στο: https://doi:10.4018/ijsppc.315591

Selinger, E., Altman, E. and Foster, S. (2023) 'Eye-Tracking in Virtual Reality A Visceral Notice Approach for Protecting Privacy', *Privacy Studies Journal*, 2, σ. 1–34. Διαθέσιμο στο: https://doi:10.7146/psj.v2i.134656

Vergara, D., Rubio, M.P. and Lorenzo, M. (2017) 'On the Design of Virtual Reality Learning Environments in Engineering', *Multimodal Technologies and Interaction*, 1(2). Διαθέσιμο στο: https://doi.org/10.3390/mti1020011

Wang, Y. *et al.* (2022) 'A survey on Metaverse: Fundamentals, Security, and Privacy', *IEEE Communications Surveys & Tutorials*, 25(1), σ. 319–352. Διαθέσιμο στο: https://doi.org/10.1109/comst.2022.3202047

Ακριβοπούλου, Χ. (2011) 'Το δικαίωμα στην προστασία των προσωπικών δεδομένων μέσα από το φακό του δικαιώματος στην ιδιωτική ζωή', *Θεωρία & Πράξη Διοικητικού Δικαίου*, 7/2011, σ. 679-691

Καρδαμάκη, Α. (2022) 'Εικονικοί Κόσμοι, Metaverse και Προστασία Δεδομένων Προσωπικού Χαρακτήρα', *Επιθεώρηση Δικαίου Πληροφορικής*, 3(1). Διαθέσιμο στο: https://doi.org/10.26262/infolawj.v3i1.8907

Καρκατζούνης, Β. και Μήτρου, Λ. (2020) 'Online διαφήμιση και προστασία προσωπικών δεδομένων', *ΔiMEE*, 1/2020, σ. 5-16

Κοντογεώργου, Π., Συρμακέζη, Ζ., Ζούλοβιτς, Μ. (2022) 'Metaverse: βασικές νομικές προκλήσεις στο νέο εικονικό σύμπαν του web3', *Συνήγορος* 151/2022, σ. 52 – 56

Κουσουνή-Πανταζοπούλου, Α. (2023) 'Metaverse και αναφυόμενα νομικά ζητήματα' *Ελληνική Δικαιοσύνη, 2/2023*, σ. 376-386

ΒΙΒΛΙΟΓΡΑΦΙΑ

Kalpokas, I. and Kalpokienė, J. (2023) *Regulating the Metaverse: A Critical Assessment*. London: Routledge

Ιγγλεζάκης, Ι. (2021) *Δίκαιο πληροφορικής*. Αθήνα-Θεσσαλονίκη: Εκδόσεις Σάκκουλα, Δ' έκδοση

Κανέλλος, Λ. (2020) *THE GDPR HANDBOOK: για DPOs, Επιχειρήσεις & Οργανισμούς.* Αθήνα: Νομική Βιβλιοθήκη

Κουσουνή-Πανταζοπούλου, Α. (2022) *Cloud Computing & νομικά ζητήματα*. Αθήνα: Νομική Βιβλιοθήκη

Παπαθανασίου, Β. (2022) *Μη εναλλάξιμα κρυπτοπαραστατικά - Non-Fungible Tokens, Νομικά ζητήματα & προτάσεις.* Αθήνα: Νομική Βιβλιοθήκη

ΝΟΜΟΘΕΣΙΑ

Σύμβαση του Συμβουλίου της Ευρώπης 108, της 28ης Ιανουαρίου 1981, για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων

Οδηγία (ΕΚ) 95/46 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Οκτωβρίου 1995, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών

Οδηγία (ΕΚ) 2002/58 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες)

Οδηγία (ΕΕ) 2015/1535 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 9ης Σεπτεμβρίου 2015, για την καθιέρωση μιας διαδικασίας πληροφόρησης στον τομέα των τεχνικών προδιαγραφών και των κανόνων σχετικά με τις υπηρεσίες της κοινωνίας των πληροφοριών

Οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, την τροποποίηση του κανονισμού (ΕΕ) αριθ. 910/2014 και της οδηγίας (ΕΕ) 2018/1972, και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148 (οδηγία NIS 2)

Πρόταση Κανονισμού (ΕΕ) του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 10ης Ιανουαρίου 2017, για τον σεβασμό της ιδιωτικής ζωής και την προστασία των δεδομένων προσωπικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες και την κατάργηση της οδηγίας 2002/58/ΕΚ (κανονισμός για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες)

Πρόταση Κανονισμού (ΕΕ) του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 21ης Απριλίου 2021, για τη θέσπιση εναρμονισμένων κανόνων σχετικά με την τεχνητή νοημοσύνη (Πράξη για την Τεχνητή Νοημοσύνη) και την τροποποίηση ορισμένων νομοθετικών πράξεων της Ένωσης

Πρόταση Κανονισμού (ΕΕ) του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 30ης Ιουνίου 2021, για τη γενική ασφάλεια των προϊόντων, την τροποποίηση του κανονισμού (ΕΕ) αριθ. 1025/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και την κατάργηση της οδηγίας 87/357/ΕΟΚ του Συμβουλίου και της οδηγίας 2001/95/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου

Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων)

Διορθωτικό στον Κανονισμό (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων)

Κανονισμός (ΕΕ) 2022/2065 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 19ης Οκτωβρίου 2022, σχετικά με την ενιαία αγορά ψηφιακών υπηρεσιών και την τροποποίηση της οδηγίας 2000/31/εκ (πράξη για τις ψηφιακές υπηρεσίες)

ΧΘΔΕΕ

ΣΛΕΕ

Σύνταγμα

Ν. 2472/1997

Ν. 4624/2019

ΓΝΩΜΕΣ-ΚΑΤΕΥΘΥΝΤΗΡΙΕΣ ΓΡΑΜΜΕΣ

Ομάδα προστασίας δεδομένων του άρθρου 29, Γνώμη 4/2007 σχετικά με την έννοια του όρου «δεδομένα προσωπικού χαρακτήρα», της 20ης Ιουνίου 2007. Διαθέσιμο στο https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_el.pdf)

Ομάδα προστασίας δεδομένων του άρθρου 29, Γνώμη 5/2009 σχετικά με τις επιγραμμικές υπηρεσίες κοινωνικής δικτύωσης, της 12ης Ιουνίου 2009. Διαθέσιμο στο: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_el.pdf)

Ομάδα προστασίας δεδομένων του άρθρου 29, Γνώμη 2/2010 σχετικά με την επιγραμμική συμπεριφορική διαφήμιση, της 22ας Ιουνίου 2010. Διαθέσιμο στο: https://www.dpa.gr/sites/default/files/2019-10/WP171_EL.PDF

Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, της 2ας Απριλίου 2013. Διαθέσιμο στο: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

Ομάδα προστασίας δεδομένων του άρθρου 29, Γνώμη 05/2014 σχετικά με τις τεχνικές ανωνυμοποίησης, της 10ης Απριλίου 2014. Διαθέσιμο στο: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_el.pdf

Ομάδα προστασίας δεδομένων του άρθρου 29, Κατευθυντήριες γραμμές σχετικά με το δικαίωμα στη φορητότητα των δεδομένων, της 5ης Απριλίου 2017. Διαθέσιμο

στο:
https://www.lawspot.gr/sites/default/files/misc/misc_legal/wp242rev01_el.pdf

Ομάδα προστασίας δεδομένων του άρθρου 29, Κατευθυντήριες γραμμές για την αυτοματοποιημένη λήψη αποφάσεων και την κατάρτιση προφίλ για τους σκοπούς του κανονισμού 2016/679, της 6ης Φεβρουαρίου 2018. Διαθέσιμο στο: https://ec.europa.eu/newsroom/article29/items/612053/en

Ομάδα προστασίας δεδομένων του άρθρου 29, Κατευθυντήριες γραμμές σχετικά με τη διαφάνεια βάσει του κανονισμού 2016/679, της 11ης Απριλίου 2018. Διαθέσιμο στο https://www.dpa.gr/sites/default/files/2020-05/wp260rev01_el.pdf

Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, Κατευθυντήριες γραμμές 3/2018 σχετικά με το εδαφικό πεδίο εφαρμογής του ΓΚΠΔ (άρθρο 3), Έκδοση 2.1, της 12ης Νοεμβρίου 2019. Διαθέσιμο στο: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_consultation_el.pdf

Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, Κατευθυντήριες γραμμές 2/2019 για την επεξεργασία δεδομένων προσωπικού χαρακτήρα σύμφωνα με το άρθρο 6 παράγραφος 1 στοιχείο β) του ΓΚΠΔ στο πλαίσιο της παροχής επιγραμμικών υπηρεσιών σε υποκείμενα δεδομένων, Έκδοση 2.0, της 8ης Οκτωβρίου 2019. Διαθέσιμο στο: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_el.pdf

Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, Κατευθυντήριες γραμμές 5/2020 σχετικά με τη συγκατάθεση βάσει του κανονισμού 2016/679, Έκδοση 1.1, της4ης Μαΐου 2020. Διαθέσιμο στο: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_el.pdf

Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, Κατευθυντήριες γραμμές 07/2020 σχετικά με τις έννοιες του υπευθύνου επεξεργασίας και του εκτελούντος την επεξεργασία στον ΓΚΠΔ, Έκδοση 2.0, της 7ης Ιουλίου 2021. Διαθέσιμο στο: https://edpb.europa.eu/system/files/2022-02/eppb_guidelines_202007_controllerprocessor_final_el.pdf

Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, Κατευθυντήριες γραμμές 8/2020 σχετικά με τη στόχευση χρηστών μέσων κοινωνικής δικτύωσης, Έκδοση 2.0, της 13ης Απριλίου

2021. Διαθέσιμο στο: https://edpb.europa.eu/system/files/2021-11/edpb_guidelines_082020_on_the_targeting_of_social_media_users_el_0.pdf

ΝΟΜΟΛΟΓΙΑ

Απόφαση ΔΕΕ C-101/01, Bodil Lindqvist, της 6ης Νοεμβρίου 2003. Διαθέσιμο στο: https://curia.europa.eu/juris/showPdf.jsf;jsessionid=CF52C9C21E43732093D105DEE15A44B1?text=&docid=48382&pageIndex=0&doclang=EL&mode=lst&dir=&occ=first&part=1&cid=14057586

Απόφαση ΔΕΕ C-293/12 και C-594/12, Digital Rights Ireland, της 8ης Απριλίου 2014. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/el/TXT/?uri=CELEX%3A62012CJ0293.

Απόφαση ΔΕΕ C-131/12, Google Spain, της 13ης Μαΐου 2014. Διαθέσιμο στο: https://curia.europa.eu/juris/document/document.jsf;jsessionid=4415E5F4881AE4B87EB3474981CBECBF?text=&docid=152065&pageIndex=0&doclang=el&mode=lst&dir=&occ=first&part=1&cid=18541420

Απόφαση ΔΕΕ C-362/14, Maximillian Schrems, της 6ης Οκτωβρίου 2015. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:62014CJ0362&from=en

Απόφαση ΔΕΕ C-582/14, Patrick Breyer, της 19ης Οκτωβρίου 2016. Διαθέσιμο στο: https://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=el&mode=lst&dir=&occ=first&part=1&cid=946993

Απόφαση ΔΕΕ C-210/16, Wirtschaftsakademie Schleswig-Holstein GmbH, της 5ης Ιουνίου 2018. Διαθέσιμο στο: https://curia.europa.eu/juris/document/document.jsf?text=&docid=202543&pageIndex=0&doclang=el&mode=lst&dir=&occ=first&part=1&cid=18623509

Απόφαση ΔΕΕ C-311/18, Maximillian Schrems, της 16ης Ιουλίου 2020. Διαθέσιμο στο https://curia.europa.eu/juris/document/document.jsf;jsessionid=699F5010F9ED77A76EF28523A1A60EE9?text=&docid=228677&pageIndex=0&doclang=EL&mode=req&dir=&occ=first&part=1&cid=10320201

ΙΣΤΟΤΟΠΟΙ - ΙΣΤΟΣΕΛΙΔΕΣ

Ball, M. (2021) 'Framework for the Metaverse — MatthewBall.vc', *MatthewBall.vc*, 29 Ιουνίου. Διαθέσιμο στο: https://www.matthewball.vc/all/forwardtothemetaverseprimer [Πρόσβαση 5 Μαΐου 2023]

Bosworth, A. and Clegg, N. (2021) 'Building the Metaverse Responsibly', *Meta*, 27 Σεπτεμβρίου. Διαθέσιμο στο: https://about.fb.com/news/2021/09/building-the-metaverse-responsibly/ [Πρόσβαση 12 Μαΐου 2023]

Castro, C. (2021) 'Tasting Digital: How the Way you Sense the World Will Change in the Next Decade', *6GWorld*, 7 Ιανουαρίου. Διαθέσιμο στο: https://www.6gworld.com/exclusives/tasting-digital-how-the-way-you-sense-the-world-will-change-by-the-time-6g-is-real/ [Πρόσβαση 12 Μαΐου 2023]

Datatron Blog (2022) *Real-life Examples of Discriminating Artificial Intelligence*. Διαθέσιμο στο: https://datatron.com/real-life-examples-of-discriminating-artificial-intelligence/[Πρόσβαση 6 Μαΐου 2023]

European Data Protection Supervisor (2023) *Metaverse.* Διαθέσιμο στο: https://edps.europa.eu/press-publications/publications/techsonar/metaverse_en [Πρόσβαση 23 Μαΐου 2023]

Garrett, U. (2023) 'Why the Meta Quest 2 is still the virtual reality headset to buy', *CNN Underscored.* 24 Ιανουαρίου. Διαθέσιμο στο: https://edition.cnn.com/cnn-underscored/reviews/oculus-quest-2 [Πρόσβαση 23 Μαΐου 2023]

Gartner (2022) *Gartner Predicts 25% of People Will Spend At Least One Hour Per Day in the Metaverse by 2026.* Διαθέσιμο στο: https://www.gartner.com/en/newsroom/press-releases/2022-02-07-gartner-predicts-25-percent-of-people-will-spend-at-least-one-hour-per-day-in-the-metaverse-by-2026 [Πρόσβαση 23 Μαΐου 2023]

Glover, E. (2022) 'Strong AI vs. Weak AI: What's the Difference?' *Built In*, 27 Οκτωβρίου. Διαθέσιμο στο: https://builtin.com/artificial-intelligence/strong-ai-weak-ai [Πρόσβαση 12 Μαΐου 2023]

Gozman, V. (2022) 'The Slow Death Of Third-Party Cookies', *Forbes*, 12 Σεπτεμβρίου. Διαθέσιμο στο: https://www.forbes.com/sites/theyec/2022/09/12/the-slow-death-of-third-party-cookies/?sh=2dd8d8644026 [Πρόσβαση 6 Μαΐου 2023]

Hamilton, I. A. (2019) 'Apple cofounder Steve Wozniak says Apple Card offered his wife a lower credit limit', *Insider*, 11 Νοεμβρίου. Διαθέσιμο στο:

https://www.businessinsider.com/apple-card-sexism-steve-wozniak-2019-11?IR=T [Πρόσβαση 6 Μαΐου 2023]

Kim, S. (2021) 'South Korea's Approach to the Metaverse', *The Diplomat*, 2 Νοεμβρίου. Διαθέσιμο στο: https://thediplomat.com/2021/11/south-koreas-approach-to-the-metaverse/ [Πρόσβαση 12 Μαΐου 2023]

Knibbeler, D., Mohrmann, M. and Zadeh, S. (2022) 'EU: Privacy and security concerns in the metaverse', Αύγουστος 2022. Διαθέσιμο στο: https://www.dataguidance.com/opinion/eu-privacy-and-security-concerns-metaverse [Πρόσβαση 12 Μαΐου 2023]

Koehler, P. (2022) 'The Metaverse and some of its emerging challenges for data protection law' *Taylor Wessing*, 10 Οκτωβρίου. Διαθέσιμο στο: https://www.taylorwessing.com/en/insights-and-events/insights/2022/10/the-metaverse-and-some-of-its-emerging-challenges-for-data-protection-law [Πρόσβαση 6 Μαΐου 2023]

Lecocq, D. and Omer, L. M. (2022) 'The Privacy, Data Protection and Cybersecurity Law Review: Metaverse and the Law' The Law Reviews, 27 Οκτωβρίου. Διαθέσιμο στο: https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/metaverse-and-the-law [Πρόσβαση 6 Μαΐου 2023]

Lumley, C. (2022) 'Data protection in the metaverse', Lexology. 27 Οκτωβρίου. Διαθέσιμο στο: https://www.lexology.com/library/detail.aspx?g=335a2e93-8ba3-46e5-9988-4c0c04b54d89 [Πρόσβαση 23 Μαΐου 2023]

Marinotti, J. (2022) 'Can you truly own anything in the metaverse? A law professor explains how blockchains and NFTs don't protect virtual property', The Conversation, 21 Απριλίου. Διαθέσιμο στο: https://theconversation.com/can-you-truly-own-anything-in-the-metaverse-a-law-professor-explains-how-blockchains-and-nfts-dont-protect-virtual-property-179067 [Πρόσβαση 12 Μαΐου 2023]

Marr, B. (2022) 'The 10 Best Metaverse Quotes Everyone Should Read', Forbes, 15 Αυγούστου. Διαθέσιμο στο: https://www.forbes.com/sites/bernardmarr/2022/08/15/the-10-best-metaverse-quotes-everyone-should-read/ [Πρόσβαση 12 Μαΐου 2023]

Meshi, D. (2022) 'The metaverse is money and crypto is king – why you'll be on a blockchain when you're virtual-world hopping', The Conversation, 14 Ιανουαρίου. Διαθέσιμο στο:

https://theconversation.com/the-metaverse-is-money-and-crypto-is-king-why-youll-be-on-a-blockchain-when-youre-virtual-world-hopping-171659 [Πρόσβαση 12 Μαΐου 2023]

Metaverse Standards Forum (2023) The Metaverse Standards Forum. Διαθέσιμο στο: https://metaverse-standards.org/ [Πρόσβαση 6 Μαΐου 2023])

Murphy, S. et al. (2021) 'The Metaverse: The evolution of a universal digital platform', *Norton Rose Fulbright*. Διαθέσιμο στο: https://www.nortonrosefulbright.com/en/knowledge/publications/5cd471a1/the-metaverse-the-evolution-of-a-universal-digital-platform [Πρόσβαση 5 Μαΐου 2023]

Ongun, C.A. (2022) 'Turkey: Evaluation On The Concepts Of Data Controller And Data Processor In The Metaverse' *Mondaq*, 22 Δεκεμβρίου. Διαθέσιμο στο: https://www.mondaq.com/turkey/data-protection/1263864/evaluation-on-the-concepts-of-data-controller-and-data-processor-in-the-metaverse#_ftn27 [Πρόσβαση 6 Μαΐου 2023]

Sanford, C. (2021) 'Meta (Facebook) Connect 2021 Metaverse Event Transcript', *Rev*, 29 Οκτωβρίου. Διαθέσιμο στο: https://www.rev.com/blog/transcripts/meta-facebook-connect-2021-metaverse-event-transcript [Πρόσβαση 5 Μαΐου 2023]

Schlemann, D. (2022) 'Metaverse Blog Series: No. 5 – Data Privacy in the Metaverse', *Arqis*, 28 Οκτωβρίου. Διαθέσιμο στο: https://www.arqis.com/en/blogs/metaverse-blog-5-data-privacy-in-the-metaverse/ [Πρόσβαση 23 Μαΐου 2023]

Tucci, L. (2023) 'What is the metaverse? An explanation and in-depth guide', *WhatIs.com*, 25 Απριλίου. Διαθέσιμο στο: https://www.techtarget.com/whatis/feature/The-metaverse-explained-Everything-you-need-to-know [Πρόσβαση 5 Μαΐου 2023]

Weingarden, G. and Artzt, M. (2022) 'Metaverse and privacy', *International Association of Privacy Professionals*, 23 Αυγούστου. Διαθέσιμο στο: https://iapp.org/news/a/metaverse-and-privacy-2/ [Πρόσβαση 23 Μαΐου 2023]

Wikipedia (2023) *Cryptocurrency*, Διαθέσιμο στο: https://en.wikipedia.org/wiki/Cryptocurrency.

Wikipedia (2023) *Internet of things*. Διαθέσιμο στο: https://en.wikipedia.org/wiki/Internet_of_things [Πρόσβαση 12 Μαΐου 2023]

Wikipedia (2023) *Smart contract*. Διαθέσιμο στο: https://en.wikipedia.org/wiki/Smart_contract [Πρόσβαση 5 Μαΐου 2023]

Wikipedia (2023) *Snow Crash*. Διαθέσιμο στο: https://en.wikipedia.org/wiki/Snow_Crash [Πρόσβαση 5 Μαΐου 2023]

Wikipedia (2023) *Virtual reality headset*. Διαθέσιμο στο: https://en.wikipedia.org/wiki/Virtual_reality_headset [Πρόσβαση 12 Μαΐου 2023]

Wikipedia (2023) *Virtual reality*. Διαθέσιμο στο: https://en.wikipedia.org/wiki/Virtual_reality [Πρόσβαση 12 Μαΐου 2023]

Zuckerberg, M. (2021) 'Founder's Letter, 2021', *Meta*, 28 Οκτωβρίου. Διαθέσιμο στο: https://about.fb.com/news/2021/10/founders-letter/ [Πρόσβαση 5 Μαΐου 2023]

Βικιπαίδεια (2022) *Άβαταρ*. Διαθέσιμο στο: https://el.wikipedia.org/wiki/%CE%86%CE%B2%CE%B1%CF%84%CE%B1%CF%81 [Πρόσβαση 6 Μαΐου 2023]

Βικιπαίδεια (2023) *Second Life*. Διαθέσιμο στο: https://el.wikipedia.org/wiki/Second_Life [Πρόσβαση 5 Μαΐου 2023])

Ευρωπαϊκή Επιτροπή (2022) *Ο Βιομηχανικός Συνασπισμός Εικονικής και Επαυξημένης Πραγματικότητας*. Διαθέσιμο στο: https://digital-strategy.ec.europa.eu/el/policies/virtual-and-augmented-reality-coalition [Πρόσβαση 12 Μαΐου 2023]

Χιόνη, Γ. (2022) 'Δίκαιο και Μετασύμπαν (II): Το δίκαιο των avatar', *Lawspot*, 12 Οκτωβρίου. Διαθέσιμο στο: https://www.lawspot.gr/nomika-blogs/georgia_hioni/dikaio-kai-metasympan-ii-dikaio-ton-avatar [Πρόσβαση 6 Μαΐου 2023]

ΕΚΘΕΣΕΙΣ-ΑΝΑΚΟΙΝΩΣΕΙΣ-ΑΠΟΦΑΣΕΙΣ &ΛΟΙΠΕΣ ΔΗΜΟΣΙΕΥΣΕΙΣ

Analysis and Research Team (ART) (2022) *Metaverse - Virtual World, Real Challenges*. Βρυξέλλες: Συμβούλιο της Ευρωπαϊκής Ένωσης. Διαθέσιμο στο: https://www.consilium.europa.eu/media/54987/metaverse-paper-9-march-2022.pdf

Citi GPS: Global Perspectives & Solutions (2022) 'Metaverse and Money Decrypting the Future'. Διαθέσιμο στο: https://ir.citi.com/gps/x5%2BFQJT3BoHXVu9MsqVRoMdiws3RhL4yhF6Fr8us8oHaOe1W9smOy1%2B8aaAgT3SPuQVtwC5B2%2Fc%3D

Clifford Chance (2022) 'The Metaverse: What are the legal implications?' Διαθέσιμο στο: https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2022/02/the-metaverse-what-are-the-legal-implications.pdf

Common Sense (n.d.) 'Kids and the Metaverse: What Parents, Policymakers, and Companies Need to Know'. Διαθέσιμο στο:

https://www.commonsensemedia.org/sites/default/files/featured-content/files/metaverse-white-paper.pdf

Deloitte Canada (n.d.) 'Welcome to the Metaverse'. Διαθέσιμο στο: https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/technology-media-telecommunications/ca-industry-tmt-welcome-to-the-metaverse-en.pdf

Directorate-General for Justice and Consumers (2020) *Algorithmic discrimination in Europe: Challenges and opportunities for gender equality and non-discrimination law.* Λουξεμβούργο: Ευρωπαϊκή Επιτροπή. Διαθέσιμο στο: https://op.europa.eu/en/publication-detail/-/publication/082f1dbc-821d-11eb-9ac9-01aa75ed71a1/language-en

European Data Protection Supervisor (2019) *Technology Report No 1: Smart glasses and data protection.* Βρυξέλλες: European Data Protection Supervisor. Διαθέσιμο στο: https://edps.europa.eu/sites/edp/files/publication/19-01-18_edps-tech-report-1-smart_glasses_en.pdf

European Parliamentary Research Service (EPRS) (2022) *Metaverse: Opportunities, risks and policy implications.* Βρυξέλλες: Ευρωπαϊκό Κοινοβούλιο. Διαθέσιμο στο: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733557/EPRS_BRI(2022)733557_EN.pdf

European Union Agency for Network and Information Security (ENISA) (2017) *Privacy and data protection in mobile applications: A study on the app development ecosystem and the technical implementation of GDPR.* Κρήτη: ENISA. Διαθέσιμο στο: https://pure.uva.nl/ws/files/42887337/22302384.pdf

GSMA Intelligence (2022) 'Exploring the metaverse and the digital future'. Διαθέσιμο στο: https://www.gsma.com/asia-pacific/wp-content/uploads/2022/02/270222-Exploring-the-metaverse-and-the-digital-future.pdf

JPMorgan Chase & Co (2022) 'Opportunities in the metaverse'. Διαθέσιμο στο: https://www.jpmorgan.com/content/dam/jpm/treasury-services/documents/opportunities-in-the-metaverse.pdf

Nextrope (2022) 'The State of The Metaverse in 2022 – Building in Open World'. Διαθέσιμο στο: https://nextrope.com/wp-content/themes/nextrope/assets/files/metaverse.pdf

Panel for the Future of Science and Technology (STOA) (2019) *Blockchain and the General Data Protection Regulation Can distributed ledgers be squared with European data protection law?* Βρυξέλλες: Ευρωπαϊκό Κοινοβούλιο. Διαθέσιμο στο:

https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf

Todd, E. et al. (2022) 'Data protection and privacy' in 'The Reed Smith Guide to the Metaverse - 2nd Edition'. Διαθέσιμο στο: https://www.reedsmith.com/en/perspectives/metaverse/2022/08/data-protection-and-privacy

Ανακοίνωση της Ευρωπαϊκής Επιτροπής, Τεχνητή Νοημοσύνη για την Ευρώπη, της 25ης Απριλίου 2018, COM (2018) 237 final, 25.04.2018

Απόφαση (ΕΕ) 2016/1250 της Ευρωπαϊκής Επιτροπής, της 12ης Ιουλίου 2016, βάσει της οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την επάρκεια της προστασίας που παρέχεται από την ασπίδα προστασίας της ιδιωτικής ζωής ΕΕ–ΗΠΑ

Απόφαση (ΕΚ) 2000/520 της Ευρωπαϊκής Επιτροπής, της 26ης Ιουλίου 2000, βάσει της οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την επάρκεια της προστασίας που παρέχεται από τις αρχές ασφαλούς λιμένα για την προστασία της ιδιωτικής ζωής και τις συναφείς συχνές ερωτήσεις που εκδίδονται από το Υπουργείο Εμπορίου των ΗΠΑ. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32000D0520

Ευρωπαϊκή Επιτροπή Ερωτήσεις & Απαντήσεις: Πλαίσιο προστασίας δεδομένων ΕΕ-ΗΠΑ, της 7ης Οκτωβρίου 2022. Διαθέσιμο στο https://www.dpa.gr/sites/default/files/2022-11/E%cf%81%cf%89%cf%84%ce%ae%cf%83%ce%b5%ce%b9%cf%82_%ce%91%cf%80%ce%b1%ce%bd%cf%84%ce%ae%cf%83%ce%b5%ce%b9%cf%82_%ce%a0%ce%bb%ce%b1%ce%af%cf%83%ce%b9%ce%bf%20%ce%a0%cf%81%ce%bf%cf%83%cf%84%ce%b1%cf%83%ce%af%ce%b1%cf%82%20%ce%94%ce%b5%ce%b4%ce%bf%ce%bc%ce%ad%ce%bd%cf%89%ce%bd%20%ce%95%ce%95-%ce%97%ce%a0%ce%91.pdf

ΔΙΠΛΩΜΑΤΙΚΕΣ ΕΡΓΑΣΙΕΣ

Καλπία, Ε. (2022) *Προστασία της ιδιωτικότητας των χρηστών των μέσων κοινωνικής δικτύωσης σε οικοσυστήματα έξυπνων κινητών*. Πειραιάς: Πανεπιστήμιο Πειραιώς