ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών

«ΔΙΚΑΙΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ»

Ακαδημαϊκό έτος 2022-2023

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ
της Μανίκα Ευαγγελίας (Α.Μ.: ΜΔΙ2123)

Metaverse και Νομικά ζητήματα: Προστασία δεδομένων, ευθύνη, ζητήματα ανταγωνισμού, ασφάλεια (Metaverse and Legal Issues: data protection, liability, competition issues, security)

Επιβλέπουσα:

Καθηγήτρια Λίλιαν Μήτρου

Πειραιάς, Ιούλιος 2023

Στην οικογένεια μου, Κώστα & Λαμπρινή,

Σταυρούλα & Γιάννη

ΠΕΡΙΛΗΨΗ

Η ταχύτατη εξέλιξη της τεχνολογίας σε συνδυασμό με τις ανάγκες των σύγχρονων ανθρώπων, ειδικότερα μετά την άφιξη της πανδημίας Covid-19, η οποία αποτέλεσε την αιτία της έντονης κοινωνικής απομόνωσης και παράλληλης ανάγκης των ανθρώπων για εξεύρεση νέων τρόπων κοινωνικής επαφής, καταστούν αναγκαία την ύπαρξη νέων τεχνολογικών δυνατότητων, μέσω των οποίων οι άνθρωποι θα δύνανται, μεταξύ άλλων, να επικοινωνούν, να κοινωνικοποιούνται καθώς και να περνούν μεγάλο μέρος της καθημερινότητας τους, υλοποιώντας μέρος των υποχρεώσεων και δραστηριοτήτων τους. Για αυτούς και πολλούς άλλους λόγους το Metaverse έχει ήδη αρχίσει εδώ και καιρό να συζητείται έντονα καθώς μέσω αυτού του νέου εικονικού κόσμου, οι μεν νέες ευκαιρίες είναι αμέτρητες, οι δε προκλήσεις έντονες.

Ειδικότερα, το metaverse μπορεί να προσφέρει μια σειρά από διευκολύνσεις στη ζωή του σύγχρονου ανθρώπου, ο οποίος δύναται να εργάζεται, να ψυχαγωγείται, να προβαίνει σε αγορές κινητών και ακινήτων πραγμάτων εντός του metaverse χρησιμοποιώντας συγκεκριμένες τεχνολογικές συσκευές μέσω των οποίων θα παρέχεται η εν λόγω μοναδική δυνατότητα και εμπειρία. Ωστόσο, το εν λόγω ψηφιακό περιβάλλον είναι βέβαιο ότι θα φέρει αντιμέτωπους τόσο τους χρήστες όσο και τους διαχειριστές με μια σειρά νομικών ζητημάτων, εκτεινόμενων από την προστασία των προσωπικών δεδομένων και την ασφάλεια έως και τη ρύθμιση του ανταγωνισμού καθώς και του καθορισμού της ευθύνης εντός του metaverse. Η παρούσα μελέτη εστιάζει στις βασικότερες πτυχές των ως άνω αναφερόμενων ζητημάτων.

ABSRACT

The rapid development of technology, combined with the demands of contemporary society and the arrival of the Covid-19 pandemic, which has led to prolonged social isolation and a simultaneous need for new forms of social interaction, has necessitated new technological means by which individuals can communicate, socialise and carry out various aspects of their daily lives, responsibilities and activities. As a result, the emergence of the Metaverse has been hotly debated, as this new virtual world offers a multitude of opportunities and challenges.

In particular, the metaverse has the potential to revolutionise the lives of modern individuals by enabling them to work, entertain themselves, travel and even purchase property within its virtual boundaries, using specialised technological devices that facilitate these unique opportunities and experiences. However, this digital environment is bound to confront both users and operators with a number of legal considerations, mainly relating to privacy, security, competition and the definition of liability within the metaverse. This study focuses on the most fundamental aspects of these issues.

ΠΕΡΙΕΧΟΜΕΝΑ

1. ΕΙΣΑΓΩΓΗ

Καταρχάς, το metaverse ως έννοια πρωτοεμφανίστηκε ήδη πριν τριάντα περίπου χρόνια, ήτοι το 1992, στο μυθιστόρημα επιστημονικής φαντασίας με τίτλο «Snow Crash» του Neal Stephenson προκειμένου να αποτυπωθεί ένας εικονικός κόσμος που βασίζεται στο διαδίκτυο και εντός του οποίου οι χρήστες μπορούν να εμφανίζονται με το άβαταρ τους και να δημιουργούν μια ψηφιακή πραγματικότητα ανταλλάσσοντας ταυτόχρονα τις εμπειρίες τους[1]. Αναφορικά ιδίως με το τι ακριβώς είναι το metaverse, πρέπει να σημειωθεί ότι δεν υφίσταται ενιαίος ορισμός που να καλύπτει την έννοια και το πλήρες φάσμα του metaverse[2], το οποίο αποτελεί εν γένει ένα «*συλλογικό εικονικό κοινόχρηστο χώρο*»[3]. Ο δε όρος metaverse συνιστά σύνθετη λέξη αποτελούμενη «*από το ελληνικό πρόθεμα μετά (Meta) και τη λέξη σύμπαν, ήτοι ένα σύμπαν μετά την πραγματικότητα*»[4].

Σήμερα, ο όρος metaverse περιλαμβάνει ιδίως την έννοια ενός «*εμβυθιστικού και μόνιμου εικονικού κόσμου*»[5] εντός του οποίου οι χρήστες έχουν τη δυνατότητα, μεταξύ άλλων, της επικοινωνίας και αλληλεπίδρασης με άλλους χρήστες καθώς και συμμετοχής σε πληθώρα κοινωνικών δραστηριοτήτων, παρόμοιων με του πραγματικού/φυσικού περιβάλλοντος. Οι εικονικοί κόσμοι στο χώρο του Διαδικτύου, όπως το metaverse αποτελούν επί της ουσίας περιβάλλοντα που «εισάγουν» τους χρήστες στην εικονική πραγματικότητα, δημιουργώντας εικονικές κοινότητες, ήτοι περιβάλλοντα στα οποία οι χρήστες νιώθουν ότι βρίσκονται φυσικά εντός αυτών των μη φυσικών κόσμων[6]. Το metaverse αποτελεί δε ένα ψηφιακό χώρο, ο οποίος προσφέρει μια «*εικονική, τρισδιάστατη, καθηλωτική και με συγκεκριμένες κινητικές δυνατότητες και δυνατότητες αφής εμπειρία*»[7], στην οποία ο χρήσης

---

[1] Floridi, L. (2022), 'Metaverse: A Matter of Experience' *Philosophy & Technology*, 35, 73. Διαθέσιμο σε: https://doi.org/10.1007/s13347-022-00568-6 (Τελευταία πρόσβαση: 06.06.2023), σελ.2

[2] Cheng, R., Wu, N., Chen S. and Han, B. (2022) "Will Metaverse Be NextG Internet? Vision, Hype, and Reality," in *IEEE Network*, vol. 36, no. 5, pp. 197-204, September/October 2022. Διαθέσιμο σε: https://ieeexplore.ieee.org/document/9877927 (Τελευταία πρόσβαση: 16.05.2023), σελ.197

[3] Γιαννακόπουλος, Κ. (2022) *Ο νεοφεουδαρχικός συνταγματισμός*, Αθήνα – Θεσσαλονίκη: Εκδόσεις Σάκκουλα, σελ.157

[4] Αποστολάτου, Χ. (2022) *Η χρήση της Meta ως μέσο προβολής marketing*, Πανεπιστήμιο Μακεδονίας, Δημοκρίτειο Πανεπιστήμιο Θράκης. Διαθέσιμο σε: https://dspace.lib.uom.gr/bitstream/2159/27802/3/ApostolatouCharikleiaMcs2022.pdf (Τελευταία πρόσβαση: 06.06.2023), σελ.12

[5] Zhu, L. (2022), *The Metaverse: Concepts and Issues for Congress*, CRS Reports. Διαθέσιμο σε: https://crsreports.congress.gov/product/pdf/R/R47224 (Τελευταία πρόσβαση: 16.05.2023), σελ.3

[6] Ιγγλεζάκης, Ι. (2022) *Το δίκαιο της ψηφιακής οικονομίας*, Αθήνα – Θεσσαλονίκη: Εκδόσεις Σάκκουλα, σελ.51

[7] Floridi, L. (2022), ό.π.

μπορεί να εισέλθει (δυνατότητα εμβύθισης)[8] με χρήση συγκεκριμένων συσκευών π.χ. γυαλιά εικονικής πραγματικότητας.

Παρατηρείται, επομένως, ότι η έννοια του metaverse δεν είναι νέα καθώς υφίσταται ήδη από τη δεκαετία του 1990 ενώ λίγα χρόνια αργότερα οι χρήστες είχαν τη δυνατότητα μέσω παιχνιδιών ηλεκτρονικών υπολογιστών *«να ζήσουν μια δεύτερη ζωή μέσω των άβαταρ τους»*[9] σε έναν εικονικό κόσμο. Ενδεικτικά, το 2003, σχεδιάστηκε ο πρώτος διαδικτυακός εικονικός κόσμος, ο Second Life, στη συνέχεια το 2015 δημιουργήθηκε το Decentreland, το οποίο χρησιμοποιεί την τεχνολογία Blockchain, το 2016 κυκλοφόρησε το Pokémon Go, μια εφαρμογή για κινητές συσκευές[10] ενώ κυκλοφόρησε ανά τα έτη και μια σειρά άλλων παιχνιδιών όπως το Fortnite της Epic Games, το Minecraft της Microsoft, το Roblox[11] κ.α. Επομένως, οι ως άνω υπάρχοντες εικονικοί κόσμοι, εντός των οποίων οι χρήστες μπορούν να πραγματοποιήσουν δραστηριότητες αντίστοιχες με αυτής της πραγματικής ζωής όπως π.χ. αγορά ρούχων, με τη χρήση συγκεκριμένης τεχνολογίας και συσκευών (VR, AR και XR)[12], συνιστούν επί της ουσίας τους προαγγέλους του metaverse με τη μορφή που τούτο εμφανίζεται προοδευτικά σήμερα, ήτοι σε μια πιο εξελιγμένη μορφή[13].

Ειδικότερα, το metaverse έχει θεωρηθεί ως το διαδίκτυο της επόμενης γενιάς (Next - G)[14], καθώς και μια προσπάθεια μετάβασης από το Web 2.0 στο Web 3.0[15], ήτοι μετάβαση από

---

[8] Cheng S., Zhang Y., Li X., et al., (2022) 'Roadmap toward the metaverse: An AI perspective' *The Innovation*, 3(5), 100293. Διαθέσιμο σε: https://www.cell.com/the-innovation/pdf/S2666-6758(22)00089-3.pdf (Τελευταία πρόσβαση: 16.05.2023), σελ.1

[9] Χιόνη, Γ. (2022) 'Δίκαιο και Μετασύμπαν (Metaverse): Προκλήσεις και νομικά ζητήματα Ι'. Διαθέσιμο σε: https://www.lawspot.gr/nomika-blogs/georgia_hioni/dikaio-kai-metasympan-metaverse-prokliseis-kai-nomika-zitimata-i (Τελευταία πρόσβαση: 13.05.2023)

[10] Bale, A.S. et al. (2022) 'A Comprehensive Study on Metaverse and Its Impacts on Humans'. *Advances in Human-Computer Interaction*, vol. 2022, Article ID 3247060. Διαθέσιμο σε: https://www.hindawi.com/journals/ahci/2022/3247060/ (Τελευταία πρόσβαση: 16.05.2023), σελ.2

[11] Gordon, M. (2022), 'The Metaverse: What are the legal implications?', *Clifford Chance*. Διαθέσιμο σε: https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2022/02/the-metaverse-what-are-the-legal-implications.pdf (Τελευταία πρόσβαση: 17.05.2023), σελ.3

[12] Οι εν λόγω έννοιες VR, AR και XR αναλύονται στο δεύτερο κεφάλαιο της παρούσας.

[13] Warin, C. and Reinhardt, D. (2022). 'Vision: Usable Privacy for XR in the Era of the Metaverse'. *2022 European Symposium on Usable Security (EuroUSEC 2022)*, σελ.111-116. Διαθέσιμο σε: https://dl.acm.org/doi/pdf/10.1145/3549015.3554212?casa_token=2rhHWgG3ZyYAAAAA:MZp5BdPuA2mm7fLhBvPGsjbNqVWWb55YfXu_nWw_R4rMADGf0O3l2c_S-5RwTGifV4A7u30jrIAS (Τελευταία πρόσβαση: 17.05.2023), σελ.112

[14] Cheng, R., Wu, N., Chen S. and Han, B. (2022), ό.π.

[15] Κόκιου, Β. (2022) 'Νομικά ζητήματα στον χώρο του Metaverse'. Διαθέσιμο σε https://www.capital.gr/me-apopsi/3635339/nomika-zitimata-ston-xoro-tou-metaverse/ (Τελευταία πρόσβαση: 13.05.2023)

ένα «*επικεντρωμένο*»[16] σε ένα αποκεντρωμένο δίκτυο ενώ συνιστά την επόμενη φάση στην εξέλιξη της ψηφιακής τεχνολογίας, μετά τον ιστό και την κινητή τηλεφωνία[17]. Κατά μία άποψη, το metaverse δεν πρόκειται για κάποια συγκεκριμένη τεχνολογία αλλά πιθανότερα πρόκειται για μια αλλαγή του υφιστάμενου τρόπου αλληλεπίδρασης των χρηστών τόσο με τις διαδικτυακές υπηρεσίες και τεχνολογικές δυνατότητες όσο και μεταξύ τους[18].

Περαιτέρω, στον εν λόγω κόσμο οι χρήστες δημιουργούν άβαταρ, τα οποία αντιπροσωπεύουν τον εαυτό του εκάστοτε χρήστη εντός του metaverse. Με αυτόν τον τρόπο, μέσω των δυνατοτήτων της επαυξημένης ή/και εικονικής πραγματικότητας, δίνεται η δυνατότητα να υφίσταται το άτομο ταυτόχρονα και στο ψηφιακό κόσμο του metaverse όσο και στον πραγματικό κόσμο[19]. Επιπλέον, μέσω της τρισδιάστατης μοντελοποίησης θα υφίσταται η δυνατότητα δημιουργίας ψηφιακών διδύμων και επομένως οι χρήστες θα μπορούν να παρουσιάζονται ψηφιακά στην ίδια κατάσταση με εκείνη του φυσικού κόσμου[20] καθώς το ψηφιακό δίδυμο ενός ατόμου δεν περιορίζεται μόνο στο να αντικατοπτρίζει ένα συγκεκριμένο άτομο αλλά αποτελεί «*μια σχεδόν σε πραγματικό χρόνο συγχρονισμένη πολυπαρουσία*», ήτοι παρουσία σε ποικίλα μέρη ταυτόχρονα, είτε σε ψηφιακά, είτε σε φυσικά περιβάλλοντα[21].

Επιπρόσθετα, το metaverse δεν διαθέτει επί του παρόντος συγκεκριμένη μορφή καθώς μπορεί να λειτουργεί τόσο σε πλατφόρμες που διαθέτουν «*κεντρική οργάνωση όσο και σε αποκεντρωμένες πλατφόρμες με περισσότερους διαχειριστές*»[22]. Το metaverse δύναται να παρέχεται τόσο από δημόσιους όσο και από ιδιωτικούς φορείς, είτε για μεμονωμένους χρήστες, είτε να λειτουργεί ως πλατφόρμα δικτύωσης[23]. Κρίσιμο ζήτημα, συνιστά, επίσης, το πώς θα κυβερνάται ο εν λόγω παγκόσμιος εικονικός κόσμος και τι επίδραση θα έχει η

---

[16] Κουσουνή-Πανταζοπούλου, Α. (2023) 'Metaverse και αναφυόμενα νομικά ζητήματα', Ελληνική Δικαιοσύνη, 2/2023, σελ. 379

[17] Floridi, L. (2022), ό.π.

[18] Zhu, L. (2022), ό.π.

[19] Κόκιου, Β. (2022), ό.π.

[20] Cheng, R., Wu, N., Chen S. and Han, B. (2022), ό.π.

[21] Maciejewski, M. (2023), *Metaverse,* Study for the JURI Committee, Policy Department for Citizens' Rights and Constitutional Affairs, European Parliament, Brussels. Διαθέσιμο σε: https://www.europarl.europa.eu/RegData/etudes/STUD/2023/751222/IPOL_STU(2023)751222_EN.pdf (Τελευταία πρόσβαση: 03.07.2023), σελ.28

[22] Καρδαμάκη, Α. (2022), 'Εικονικοί Κόσμοι, Metaverse και Προστασία Δεδομένων Προσωπικού Χαρακτήρα', *Επιθεώρηση Δικαίου Πληροφορικής*, Τόμ. 3, Αρ. 1. Διαθέσιμο σε: https://ejournals.lib.auth.gr/infolawj/article/view/8907 (Τελευταία πρόσβαση: 15.05.2023), σελ.9

[23] Maciejewski, M. (2023), ό.π., σελ.11

ύπαρξη τοπικών κανόνων[24]. Επίσης, το metaverse σε αντιστοιχία με τη μορφή του διαδικτύου, ήτοι ιστός και επιμέρους ιστοσελίδες, πιθανότατα θα παρουσιάζεται ως metaverse και επιμέρους ιστοσελίδες του metaverse[25] π.χ. θα υπάρχει metaverse παιχνιδιών και metaverse αγορών ρούχων και άρα επιμέρους metaverses.

Αξίζει να σημειωθεί ότι πρόσφατα, τον Οκτώβριο του 2021, η εταιρεία Facebook του Mark Zuckerberg μετονομάστηκε σε Meta, κάτι το οποίο αναδεικνύει το όραμά της για την εξέλιξη του ιστού στη μορφή του metaverse με τη χρήση εκ μέρους των χρηστών τεχνολογιών, όπως η XR[26]. Στο πλαίσιο αυτό, ο Mark Zuckerberg και άλλοι δραστηριοποιούμενοι στον τομέα της τεχνολογίας ευελπιστούν ότι στο metaverse οι άνθρωποι θα ζουν και θα νιώθουν σαν να βρίσκονται στο σπίτι τους[27]. Άλλωστε, ορισμένα στελέχη της εταιρείας Meta θεωρούν ότι το metaverse δεν θα συσταθεί μόνο από μία εταιρεία, αλλά τουναντίον από περισσότερες εταιρείες, οι οποίες θα συμβάλλουν η καθεμία με ξεχωριστά δομικά στοιχεία με απώτατο σκοπό τη διαλειτουργικότητα μεταξύ των διαφορετικών στοιχείων των λοιπών εταιρειών[28].

Επομένως, μέσω του metaverse οι άνθρωποι θα μεταφέρονται εικονικά σε ένα άλλο σύμπαν, σε ένα «δεύτερο σύμπαν», το οποίο θα ομοιάζει με το φυσικό κόσμο και το φυσικό περιβάλλον και το οποίο, όμως, πέρα από τις δυνατότητες που μπορεί να προσφέρει, κρύβει και μια σειρά από κινδύνους. Ειδικότερα, τίθεται σε μεγάλο βαθμό το ζήτημα του πώς διασφαλίζεται η προστασία των προσωπικών δεδομένων των χρηστών – των άβαταρ- ενώ κρίσιμη είναι και η ασφάλεια εντός του metaverse, τόσο με την έννοια της κυβερνοασφάλειας (cybersecurity) όσο και με την έννοια της πραγματικής ασφάλειας από την άποψη διαφόρων ποινικών αδικημάτων/εγκλημάτων, τα οποία δύνανται να λάβουν χώρα εντός του metaverse.

Άλλωστε, απαραίτητος κρίνεται και ο καθορισμός του ποιος τελικά θα έχει την ευθύνη για τις διάφορες καταστάσεις, οι οποίες ενδέχεται να ανακύψουν εντός του metaverse,

---

[24] 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)*, Bologna, Italy, pp. 272-277. Διαθέσιμο σε: https://arxiv.org/pdf/2204.01480.pdf (Τελευταία πρόσβαση: 17.05.2023), σελ.275

[25] Floridi, L. (2022), ό.π.

[26] Warin, C. and Reinhardt, D. (2022), ό.π. σελ.111

[27] Gorichanaz, T. (2022), 'Being at home in the metaverse? Prospectus for a social imaginary', *AI and Ethics* 3, pp. 647–658. Διαθέσιμο σε: https://link.springer.com/article/10.1007/s43681-022-00198-w (Τελευταία πρόσβαση: 17.05.2023), σελ.654

[28] Zhu, L. (2022), ό.π., σελ.4

συμπεριλαμβανομένων των τυχόν αδικημάτων λαμβάνοντας υπόψιν τις προεκτάσεις που αναμένεται να λάβει το metaverse στην καθημερινότητα των πολιτών τα επόμενα χρόνια. Περαιτέρω, η ρύθμιση του ανταγωνισμού μεταξύ των μεγάλων πλατφορμών/παρόχων ψηφιακών υπηρεσιών κρίνεται πλέον αναγκαία σε ευρωπαϊκό επίπεδο και στο πεδίο του metaverse προκειμένου να προστατευτεί επαρκώς ο τομέας του ανταγωνισμού και στο περιβάλλον του metaverse.

Ως εκ τούτου, στην παρούσα μελέτη θα γίνει μια προσπάθεια να αναλυθούν αφενός τα βασικά χαρακτηριστικά και όλες οι κύριες δυνατότητες που προσφέρει το metaverse καθώς και το αν υπάρχει σαφές νομοθετικό πλαίσιο που να ρυθμίζει το metaverse. Αφετέρου θα εξεταστούν τα ζητήματα που ανακύπτουν εξ αφορμής του metaverse στο πεδίο των προσωπικών δεδομένων καθώς και οι τιθέμενοι κίνδυνοι, οι προκλήσεις αλλά και οι τρόποι με τους οποίους θα μπορούσαν οι εν λόγω καταστάσεις να επιλυθούν. Επιπλέον, θα αναλυθεί το ποιος μπορεί να φέρει την ευθύνη σε καταστάσεις που ανακύπτουν στο metaverse και ιδίως αν ένα άβαταρ είναι ικανό να θεωρηθεί υπεύθυνο για τις πράξεις του εντός του metaverse ή αν υπεύθυνη μπορεί να θεωρηθεί η εταιρεία πάροχος του metaverse. Άλλωστε, ειδική αναφορά θα γίνει στα ζητήματα ανταγωνισμού και κυρίως στο αν συμπεριφορές, όπως κατάχρηση δεσπόζουσας θέσης, θα μπορούσαν να εμφανιστούν και στο metaverse ενώ κρίνεται απαραίτητη και η αναφορά στην Πράξη για τις Ψηφιακές Αγορές και το πώς αυτή θα μπορούσε να εφαρμοστεί στο metaverse. Τέλος, θα μελετηθούν τα διάφορα ζητήματα ασφαλείας, τόσο εξ απόψεως κυβερνοασφαλείας όσο και εξ απόψεως των διαφόρων ποινικών αδικημάτων που δύνανται να λάβουν χώρα στο metaverse θέτοντας το κρίσιμο ερώτημα του κατά πόσον ένας χρήστης θα μπορεί να δρα με ασφάλεια εντός του metaverse καθώς και ποιες θα μπορούσαν να ήταν οι βασικές δικλείδες ασφάλειας του εντός του εν λόγω περιβάλλοντος.

2. METAVERSE - ΒΑΣΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ, ΔΥΝΑΤΟΤΗΤΕΣ ΚΑΙ ΝΟΜΟΘΕΤΙΚΟ ΠΛΑΙΣΙΟ

2.1. Γενικά: Βασικά χαρακτηριστικά και χρήση σύγχρονων τεχνολογιών εντός του Metaverse

Το metaverse συνιστά, όπως προειπώθηκε, έναν εικονικό κόσμο, στον οποίο δύναται κάποιος να εμβυθιστεί και επομένως ένα από τα πρώτα στοιχεία που χαρακτηρίζουν το metaverse είναι η εμβύθιση των ατόμων εντός του ψηφιακού τούτου κόσμου με τη χρήση των κατάλληλων τεχνολογικών συσκευών και προγραμμάτων π.χ. με τη χρήση κράνων εικονικής πραγματικότητας (HMD), είτε με τη χρήση γυαλιών 3D[29]. Άλλο ένα χαρακτηριστικό, το οποίο διαθέτουν οι υπηρεσίες του metaverse είναι και η μόνιμη πρόσβαση στο δίκτυο σε πραγματικό χρόνο, ήτοι το εικονικό περιβάλλον να συνεχίζει να υφίσταται και αφότου ο χρήστης έχει ολοκληρώσει τη χρήση του, κάτι το οποίο βεβαίως απαιτεί ικανές τεχνολογικές υποδομές, οι οποίες θα μπορούσαν να υποστηρίξουν την εν λόγω δυνατότητα π.χ. δίκτυα χαμηλής καθυστέρησης[30] όπως το 5G (δίκτυο πέμπτης γενιάς) και το 6G (δίκτυο επόμενης γενιάς)[31]. Σημειωτέον, ωστόσο, ότι υπάρχει μεγάλη πιθανότητα η μεν υφιστάμενη τεχνολογία 5G αν και αρκετά εξελιγμένη να μην είναι αρκετή για να υποστηρίξει πλήρως το metaverse[32], η δε τεχνολογία 6G επί του παρόντος τοποθετείται σε αρχικές φάσεις έρευνας και ανάπτυξης[33]. Ένα πλήρως δε λειτουργικό και εμβυθιστικό περιβάλλον metaverse απαιτεί «*αύξηση της υπολογιστικής απόδοσης κατά 1.000 φορές σε σχέση με το σημερινό επίπεδο της τεχνολογίας*»[34] και συνεπώς μεγαλύτερη κατανάλωση ενέργειας.

Η δε χρήση τεχνολογιών εντός του metaverse, όπως το cloud computing και το edge computing δύνανται να ενισχύσουν «*την ανάπτυξη της υπολογιστικής ισχύος σε κάποιο βαθμό και να γίνουν η κύρια υποδομή του metaverse*»[35], ενώ δομικό στοιχείο του metaverse συνιστά και το Διαδίκτυο των Πραγμάτων (IoT), το οποίο περιλαμβάνει όλες τις έξυπνες συσκευές καθώς συνεχώς νέες συσκευές μπορούν να συνδεθούν στο διαδίκτυο, έχοντας λάβει συγκεκριμένα ερεθίσματα του πραγματικού κόσμου μέσω αισθητήρων και συλλέγοντας πληροφορίες, τις

[29] Καρδαμάκη, Α. (2022), ό.π., σελ.3-4
[30] Zhu, L. (2022), ό.π., σελ.5
[31] Zhu, L. (2022), ό.π., σελ.13
[32] Cheng, R., Wu, N., Chen S. and Han, B. (2022), ό.π., σελ. 203
[33] Zhu, L. (2022), ό.π., σελ. 14
[34] Maciejewski, M. (2023), ό.π., σελ. 18
[35] Αποστολάτου, Χ. (2022), ό.π. σελ. 33

οποίες μεταφέρουν σε συγκεκριμένες εφαρμογές μέσω των δικτύων και με σκοπό, μεταξύ άλλων, την πιο αποδοτική λειτουργία τους[36].

Επιπλέον, η διαλειτουργικότητα αποτελεί ένα ακόμα βασικό χαρακτηριστικό του metaverse, η οποία παρέχει τη δυνατότητα αλληλεπίδρασης και ανταλλαγής πληροφοριών μεταξύ των διαφόρων συστημάτων και πλατφορμών[37]. Η εν λόγω δυνατότητα επιτρέπει επί της ουσίας στους χρήστες να μεταφέρουν τόσο τα άβαταρ τους όσο και ψηφιακά περιουσιακά στοιχεία καθώς και άλλα δεδομένα τους μεταξύ των επιμέρους εφαρμογών του metaverse ανεξαρτήτως του αν οι εν λόγω εφαρμογές είναι υπό κοινή ιδιοκτησία ενώ παράλληλα επιτυγχάνεται η διατήρηση της ταυτότητας του χρήστη καθώς και η κυριότητα επί των εν λόγω αντικειμένων, κάτι το οποίο μπορεί να εκπληρωθεί και μέσω της τεχνολογίας blockchain[38], η οποία συνιστά το κλειδί για την ασφάλεια των ψηφιακών περιουσιακών στοιχείων[39].

Όσον αφορά, ειδικότερα, στην τεχνολογία blockchain, υποστηρίζεται ότι είναι απαραίτητη η χρήση της εντός του metaverse καθώς μέσω των κρυπτονομισμάτων, τα οποία βασίζονται στην τεχνολογία blockchain και δύνανται να αποτελέσουν τον πιο πιθανό τρόπο πληρωμής εντός του metaverse, θα διευκολυνθεί η πραγματοποίηση των διαδικτυακών συναλλαγών γρήγορα, με ασφάλεια και αξιοπιστία χωρίς να υφίσταται κεντρικό εποπτικό όργανο[40]. Άλλωστε, το metaverse θα παρέχει μια μεγάλη αγορά τόσο φυσικών όσο και εικονικών αντικειμένων, τα οποία θα συνδέονται με τα άβαταρ και θα μπορούν να υλοποιηθούν ως NFTs (Non-Fungible Tokens)[41], τα οποία αντιπροσωπεύουν ψηφιακά περιουσιακά στοιχεία[42], ήτοι την ιδιοκτησία εικονικών αντικειμένων π.χ. ακινήτων,

---

[36] Κουσουνή-Πανταζοπούλου, Α. (2023), ό.π. σελ. 378

[37] Madiega, T., Car, P. et al., (2022), *Metaverse Opportunities, risks and policy implications*, European Parliamentary Research Service (EPRS). Διαθέσιμο σε: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733557 (Τελευταία πρόσβαση: 20.05.2023), σελ. 2

[38] Gordon, M. (2022), ό.π., σελ.2

[39] Cheng, R., Wu, N., Chen S. and Han, B. (2022), ό.π., σελ.198

[40] Zhu, L. (2022), ό.π., σελ.15

[41] Pietro, Di 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)*, Atlanta, GA, USA, pp. 281-288. Διαθέσιμο σε: https://ieeexplore.ieee.org/document/9750221 (Τελευταία πρόσβαση: 10.06.2023), σελ.281

[42] Zhu, L. (2022), ό.π., σελ.116

πιστοποιώντας την ταυτότητά τους[43]. Εντός του metaverse μπορεί να γίνει και χρήση έξυπνων συμβολαίων (smart contracts), τα οποία συμβάλλουν στην «*αυτοματοποιημένη εκτέλεση συναλλαγών*»[44].

Περαιτέρω, πέρα από την τεχνολογία blockhain, άλλη μια σημαντική τεχνολογία που επιτρέπει στο έπακρο τη λειτουργία του metaverse είναι η εκτεταμένη πραγματικότητα (Extended Reality - XR), η οποία συνιστά «*όρο ομπρέλα*»[45] καθώς συμπεριλαμβάνει και μια σειρά άλλων τεχνολογιών δυνατότητας επέκτασης της πραγματικότητας με την προσθήκη ψηφιακών στοιχείων στο περιβάλλον που εντοπίζεται ο χρήστης. Ειδικότερα, οι τεχνολογίες XR «*περιλαμβάνουν ένα εκτεταμένο φάσμα τεχνολογιών εμβύθισης, από την επαυξημένη πραγματικότητα (Augmented Reality -AR) έως τη μικτή πραγματικότητα (Mixed Reality - MR) και την εικονική πραγματικότητα (Virtual Reality - VR)*»[46]. Μέσω της τεχνολογίας XR καθίσταται πλήρως αληθοφανής η εμβύθιση του χρήστη εντός του metaverse[47].

Η δε τεχνολογία AR «*ενισχύει τα αντικείμενα του πραγματικού κόσμου και τα ζωντανεύει μέσω γραφικών που δημιουργούνται από υπολογιστή, δημιουργώντας μια διαδραστική εμπειρία χρήστη*»[48], υφίσταται δε μια επικάλυψη της ψηφιακής και φυσικής πραγματικότητας[49]. Επιτρέπει, επί της ουσίας, με αυτόν τον τρόπο τη «*στενή ενσωμάτωση του εικονικού και του φυσικού κόσμου*»[50], που μπορεί να κυμαίνεται από μια απλή δυνατότητα προβολής πληροφοριών έως και την προσθήκη εικονικών αντικειμένων ενώ η πρόσβαση στην εν λόγω λειτουργία πραγματοποιείται με συσκευές, όπως έξυπνα κινητά τηλέφωνα που διαθέτουν κάμερα[51]. Για παράδειγμα, η εφαρμογή Pokémon Go χρησιμοποιεί την τεχνολογία AR[52].

---

[43] Dwivedi, K. Y. et al. (2022), *Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy,* International Journal of Information Management, Volume 66. Διαθέσιμο σε: https://www.sciencedirect.com/science/article/pii/S0268401222000767 (Τελευταία πρόσβαση: 10.06.2023), σελ.9

[44] Αποστολάτου, Χ. (2022), ό.π., σελ.29

[45] Zhu, L. (2022), ό.π., σελ. 7

[46] Plechatá, A., Makransky, G. and Böhm, R. (2022) 'Can extended reality in the metaverse revolutionise health communication?', *npj Digital Medicine*, 5, 132. Διαθέσιμο σε: https://doi.org/10.1038/s41746-022-00682-x (Τελευταία πρόσβαση: 11.06.2023), σελ. 1

[47] Dwivedi, K. Y. et al. (2022), ό.π., σελ. 2

[48] Bale, A.S. et al. (2022), ό.π., σελ. 2

[49] Floridi, L. (2022), ό.π., σελ. 3

[50] Pietro, Di R., and Cresci, S. (2021), ό.π., σελ. 281

[51] Zhu, L. (2022), ό.π., σελ. 12

[52] Bale, A.S. et al. (2022), ό.π., σελ. 2

Αντιθέτως, η τεχνολογία VR δημιουργεί καθηλωτικούς τρισδιάστατους χώρους[53] που επιτρέπουν στο χρήστη να αλληλεπιδρά με ένα προσομοιωμένο εικονικό περιβάλλον[54], το οποίο έχει σχεδιαστεί από υπολογιστή και το οποίο αναπαράγει, είτε τον φυσικό, είτε ένα φανταστικό κόσμο[55] με τη χρήση π.χ. λογισμικών και ηλεκτρονικών παιχνιδιών, όπως επί παραδείγματι το Second Life[56]. Βασικό μειονέκτημα, ωστόσο, της εν λόγω εξ' ολοκλήρου ψηφιακής[57] τεχνολογίας συνιστούν οι τεχνικές προκλήσεις, δηλαδή η εμπειρία που βιώνει ο χρήστης μοιάζει σε έναν βαθμό μη φυσική ενώ μπορεί να δημιουργηθούν και άλλα ζητήματα, όπως πονοκέφαλος στο χρήστη μετά την χρήση των εν λόγω συσκευών[58]. Περαιτέρω, η τεχνολογία MR επιτρέπει στους χρήστες να αλληλεπιδρούν με εικονικά αντικείμενα που εμφανίζονται στο πραγματικό περιβάλλον, ήτοι μια αλληλεπίδραση του χρήστη και με ψηφιακά και φυσικά στοιχεία, δημιουργώντας με αυτόν τον τρόπο ένα υβριδικό περιβάλλον[59], στο οποίο κυριαρχεί η συνύπαρξη των ψηφιακών και φυσικών αντικειμένων[60].

Επιπλέον, είναι πολύ πιθανό να γίνεται εκτεταμένη χρήση της τεχνητής νοημοσύνης εντός του metaverse, σε συνδυασμό με τη χρήση αλγορίθμων μηχανικής μάθησης και αρχιτεκτονικών βαθιάς μάθησης[61]. Σημειωτέον δε, ότι η χρήση τεχνητής νοημοσύνης εντός του metaverse δύναται να ενισχύσει το ρεαλιστικό στοιχείο, όπως επί παραδείγματι, την εμφάνιση των άβαταρ, ώστε να μοιάζουν πιο ρεαλιστικά[62].

2.2. Κύριες δυνατότητες του Metaverse

Το metaverse διαδραματίζει, ιδίως μετά την άνθηση του 5G[63], σπουδαίο ρόλο σε πάρα πολλούς τομείς, από τον ακαδημαϊκό και εκπαιδευτικό χώρο μέχρι τη βιομηχανία[64]. Ειδικότερα, το metaverse μπορεί να ενισχύσει τις δυνατότητες επικοινωνίας με άλλους

[53] Pietro, Di R., and Cresci, S. (2021), ό.π.
[54] Bale, A.S. et al. (2022), ό.π., σελ. 2
[55] Zhu, L. (2022), ό.π., σελ. 11
[56] Bale, A.S. et al. (2022), ό.π., σελ. 2
[57] Floridi, L. (2022), ό.π., σελ. 3
[58] Zhu, L. (2022), ό.π., σελ. 12
[59] Zhu, L. (2022), ό.π., σελ.9
[60] Floridi, L. (2022), ό.π., σελ.3
[61] Madiega, T., Car, P. et aI., (2022), ό.π., σελ.6
[62] Αποστολάτου, Χ. (2022), ό.π. σελ. 28
[63] Cheng, R., Wu, N., Chen S. and Han, B. (2022), ό.π., σελ.197
[64] Cheng S., Zhang Y., Li X., et al., (2022), ό.π., σελ.1

χρήστες, την αγορά κινητών και ακίνητων εικονικών πραγμάτων με τη χρήση NFT's και κρυπτονομισμάτων, τη ψυχαγωγία[65] π.χ. τη διοργάνωση εικονικών συναυλιών, την αγορά ψηφιακών ειδών, την τέχνη[66], την εικονική επίσκεψη τουριστικών χώρων και ψηφιακών βιβλιοθηκών, τη διοργάνωση επαγγελματικών συναντήσεων, την ανταλλαγή χρημάτων και ψηφιακών ειδών[67], την ιατρική[68], την υλικοτεχνική υποστήριξη, μηχανική και μεταποίηση[69], τις δικαστικές διαδικασίες[70], την εξέλιξη του μάρκετινγκ ή προώθηση πωλήσεων κ.α. Για παράδειγμα, η Siemens μέσω του metaverse αξιολογεί τις αντιδράσεις των εν δυνάμει πελατών της σε προϊόντα της, τα οποία βρίσκονται σε τρισδιάστατη μορφή εντός του metaverse[71]. Ο δε χρήστης θα μπορεί να εντοπίζει εντός του metaverse και να συναλλάσσεται με κάθε επιχείρηση του φυσικού κόσμου[72]. Περαιτέρω το metaverse δύναται να ενισχύσει τον τουρισμό καθώς μπορεί να φέρει εικονικά σε επαφή τον χρήστη με μια σειρά πληροφοριών π.χ. για μνημεία πολιτιστικής κληρονομιάς και κουλτούρας[73]. Ο δημόσιος τομέας έχει τη δυνατότητα, επίσης, να χρησιμοποιήσει το metaverse «*για να παρέχει εικονικές διαβουλεύσεις και δημόσιες υπηρεσίες*»[74] ενώ ήδη μεταξύ των περιπτώσεων εμφάνισης του metaverse στο δημόσιο τομέα αποτελεί η δημιουργία του εικονικού δημαρχείου της Σεούλ, το οποίο περιλαμβάνεται στο πενταετές «Βασικό σχέδιο Metaverse της Σεούλ»[75].

Αναφορικά με τη χρήση του metaverse στον τομέα της υγείας, αξίζει να σημειωθεί ότι μπορεί να ενισχύσει την εξάλειψη των ανισοτήτων που υφίστανται στον εν λόγω τομέα, κυρίως λόγω του ότι πολλές κοινωνικές ομάδες παγκοσμίως δεν έχουν πρόσβαση σε ορθή και κατανοητή πληροφόρηση περί της υγείας αλλά και σε κατάλληλες υποδομές υγείας. Μέσω του metaverse και με τη συνδρομή των κατάλληλων συσκευών XR θα μπορούν πολίτες αναπτυσσόμενων χωρών να υποστηρίζονται στον τομέα της υγείας ενώ η πληροφορία θα μπορεί να είναι σε τέτοια μορφή, ώστε να αποτυπώνεται με άμεσο και κατανοητό τρόπο το

---

[65] Καρδαμάκη, Α. (2022), ό.π., σελ. 6
[66] Maciejewski, M. (2023), ό.π., σελ. 40
[67] Cheng S., Zhang Y., Li X., et al., (2022), ό.π., σελ.2
[68] Καρδαμάκη, Α. (2022), ό.π., σελ.6
[69] Ευρωπαϊκή Επιτροπή (2023), *Εικονικοί Κόσμοι κατάλληλοι για τους ανθρώπους.* Διαθέσιμο σε: https://digital-strategy.ec.europa.eu/el/policies/virtual-worlds (Τελευταία πρόσβαση: 14.07.2023)
[70] Maciejewski, M. (2023), ό.π., σελ. 139
[71] Ιγγλεζάκης Ι. (2022), ό.π., σελ.52
[72] Κουσουνή-Πανταζοπούλου, Α. (2023), ό.π. σελ. 379
[73] Dwivedi, K. Y. et al. (2022), ό.π., σελ.29
[74] Petrányi, D., Horváth, K. and Domokos, M. (2022) 'Legal issues in the metaverse / Part 1 - Introduction to the metaverse'. Διαθέσιμο σε: https://cms-lawnow.com/en/ealerts/2022/07/legal-issues-in-the-metaverse-part-1-introduction-to-the-metaverse (Τελευταία πρόσβαση: 11.06.2023)
[75] Maciejewski, M. (2023), ό.π., σελ. 36

πώς πρέπει να διαφυλάσσεται η υγεία του ατόμου π.χ. ο χρήστης να λαμβάνει τη θέση ενός άβαταρ που νοσεί από μια πάθηση και με αυτόν τον τρόπο να κατανοεί τη χρησιμότητα της διαφύλαξης της υγείας του. Άλλωστε θα μπορούσε να συμβάλλει δυναμικά και στη δημιουργία πιο προσωποποιημένων εμπειριών στο πλαίσιο της ιατρικής για ένα χρήστη[76] άρα να συνδράμει στην προσωποποιημένη ιατρική (personalized medicine) καθώς και να συνδράμει θετική στον τομέα της ψυχικής υγείας[77]. Επιπρόσθετα, με τη χρήση της βαθιάς μάθησης (deep learning) της τεχνητής νοημοσύνης καθίσταται δυνατό για τις συσκευές τεχνητής νοημοσύνης να *μαθαίνουν από τεράστιες ποσότητες δεδομένων*[78], κάτι το οποίο θα μπορεί να λαμβάνει χώρα και στο metaverse και ως εκ τούτου θα ήταν πολύ χρήσιμο σε τομείς, όπως η υγεία και σε συνδυασμό με τη χρήση ψηφιακών διδύμων να συμβάλλει το metaverse ενεργά και στην επίλυση τέτοιου είδους ζητημάτων π.χ. διενέργεια εξ αποστάσεως επέμβασης με τη βοήθεια του ψηφιακού διδύμου.

Περαιτέρω, το metaverse μπορεί να λειτουργήσει, είτε ως εργαλείο, ήτοι ως μέσο, το οποίο μπορεί να επιλύσει μια σειρά πραγματικών προβλημάτων της καθημερινότητας του φυσικού κόσμου, είτε ως στόχος, δηλαδή το ίδιο να αποτελεί το επίκεντρο ενεργειών, όπως αποκόμιση κέρδους εντός του metaverse. Μέσω του metaverse απλοποιούνται σύνθετες εργασίες του πραγματικού κόσμου καθώς πολλές σύνθετες δραστηριότητες π.χ. η μηχανική αεροσκαφών μπορούν να διεξαχθούν με απλό τρόπο μέσω αυτού, ενώ εργασίες κοστοβόρες μπορούν να πραγματοποιηθούν με μικρότερο κόστος[79].

Πέρα από πρακτικές εφαρμογές, το metaverse μπορεί να διαδραματίσει σημαντικό ρόλο σε ουσιαστικά κοινωνικά ζητήματα, όπως η προσβασιμότητα, επιτρέποντας, επί παραδείγματι, τη παγκόσμια συνεργασία, την εξάλειψη των συνόρων καθώς και τη διενέργεια πολλών δραστηριοτήτων π.χ. συναυλιών χωρίς να επηρεάζει η πραγματική απόσταση ενώ μπορεί να ενισχύσει την ποικιλομορφία και την ανθρωπιά[80]. Δύναται, επίσης, το metaverse, να ενισχύσει τις αρχές της ισότητας καθώς ο κάθε χρήστης μπορεί να προσαρμόσει τον εικονικό του εαυτό, το άβατάρ του, όπως ο ίδιος επιθυμεί χωρίς να τον ενδιαφέρει π.χ. το φύλο ή η κοινωνική του υπόσταση. Περαιτέρω, σημαντικές αξίες στο

[76] Plechatá, A., Makransky, G. and Böhm, R. (2022), ό.π., σελ.3
[77] Maciejewski, M. (2023), ό.π., σελ. 38
[78] Cheng, R., Wu, N., Chen S. and Han, B. (2022), ό.π., σελ.198
[79] Dwivedi, K. Y. et al. (2022), ό.π., σελ. 7
[80] Fernandez, C.B and Hui, P. (2022), ό.π., σελ. 276

metaverse αποτελούν η συνεργασία και η επικοινωνία καθώς οι χρήστες μέσω των αβατάρ τους μπορούν να επικοινωνούν και συνεργάζονται ανεξαρτήτως του τόπου και του χρόνου[81].

Άλλωστε το metaverse σταδιακά είναι ικανό να παρέχει όλες τις ως άνω δυνατότητες, τις οποίες δεν μπορούσε να προσφέρει η προηγούμενη του μορφή π.χ. Second Life, λόγω του ότι η χρήση νέων τεχνολογιών δημιουργεί πιο φυσικά αποτελέσματα κατά την εμβύθιση, είναι δε προσβάσιμο πλέον και από κινητές συσκευές ενώ έχει μεγαλύτερη απόδοση στον οικονομικό τομέα λόγω της χρήσης blockchain και κρυπτονομισμάτων[82]. Ιδανικά στο μέλλον στόχος είναι οι χρήστες πέρα από την αίσθηση παρουσίας σε ένα χώρο, να μπορούν να χρησιμοποιούν και τις αισθήσεις της όσφρησης και της γεύσης[83].

2.3. Νομοθετικό πλαίσιο

Καταρχάς πρέπει να σημειωθεί ότι δεν υφίσταται συγκεκριμένο νομοθετικό πλαίσιο που να εφαρμόζεται αποκλειστικά και μόνο στο metaverse και να προβαίνει σε αντίστοιχη αναλυτική ρύθμιση τούτου. Άλλωστε η Ευρωπαϊκή Επιτροπή δεν έχει στις άμεσες βλέψεις της την πρόταση νέων κανονιστικών μέτρων και πολιτικών αναφορικά με το metaverse καθώς θεωρεί δεδομένο ότι το υπάρχον νομοθετικό πλαίσιο εφαρμόζεται κανονικά και στο metaverse, όπως για παράδειγμα η Πράξη για τις Ψηφιακές Υπηρεσίες (εφεξής ως «DSA»)[84] και η Πράξη για τις Ψηφιακές Αγορές (εφεξής ως «DMA»)[85], οι οποίες παρέχουν τις κατάλληλες προβλέψεις και δύνανται να εφαρμοστούν και στο metaverse.

Περαιτέρω, εφόσον χρησιμοποιείται τεχνητή νοημοσύνη σε περιβάλλοντα του metaverse θα μπορούσε να τύχει εφαρμογής και η Πράξη για την Τεχνητή Νοημοσύνη (εφεξής ως «AI

---

[81] Dwivedi, K. Y. et al. (2022), ό.π., σελ. 4

[82] Dwivedi, K. Y. et al. (2022), ό.π., σελ. 4

[83] Cheng, R., Wu, N., Chen S. and Han, B. (2022), ό.π., σελ.199

[84] *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).* Διαθέσιμο σε https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:32022R2065 (Τελευταία πρόσβαση: 11.06.2023)

[85] *Κανονισμός (ΕΕ) 2022/1925 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 14ης Σεπτεμβρίου 2022 σχετικά με διεκδικήσιμες και δίκαιες αγορές στον ψηφιακό τομέα και για την τροποποίηση των οδηγιών (ΕΕ) 2019/1937 και (ΕΕ) 2020/1828 (Πράξη για τις Ψηφιακές Αγορές).* Διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/ELL/TXT/?uri=uriserv%3AOJ.L_.2022.265.01.0001.01.ELL&toc=OJ%3AL%3A2022%3A265%3ATOC (Τελευταία πρόσβαση: 11.06.2023)

Act»)[86], η οποία θα μπορούσε να προβεί σε ρύθμιση της χρήσεως π.χ. βιομετρικών δεδομένων εντός του metaverse[87] ενώ θα τύχουν απαγόρευσης συγκεκριμένες πρακτικές στο πλαίσιο της τεχνητής νοημοσύνης με την ταυτόχρονη απαίτηση των παρόχων καθώς και των χρηστών να συμμορφώνονται με συγκεκριμένες υποχρεώσεις, όπως οι προβλεπόμενες υποχρεώσεις αναφορικά με συστήματα τεχνητής νοημοσύνης υψηλού κινδύνου[88]. Θα μπορούσε δε να εφαρμοστεί και η Οδηγία περί της ευθύνης για την ΤΝ (Ai Liability Directive)[89], η οποία εφόσον υιοθετηθεί, θα μπορούσε να επιλύσει ζητήματα ευθύνης που δύνανται να ανακύψουν εξ αφορμής συστημάτων τεχνητής νοημοσύνης με σκοπό τη διευκόλυνση των χρηστών ιδίως ως προς τα ζητήματα απόδειξης.

Επίσης, θα μπορούσε να τύχει εφαρμογής και ο Γενικός Κανονισμός για την Προστασία Δεδομένων (εφεξής ως «GDPR»)[90] αναφορικά με την προστασία των προσωπικών δεδομένων των χρηστών ενώ στο πλαίσιο της κυβερνοασφάλειας, ήδη η υπάρχουσα νομοθεσία θεωρείται ελλιπής[91] αναφορικά με τα εγκλήματα που διαδραματίζονται στον κυβερνοχώρο, κάτι το οποίο θα συνιστά ακόμα μεγαλύτερο πρόβλημα εντός του metaverse λόγω των ευρέων δυνατοτήτων του που μπορεί να οδηγήσουν σε περισσότερες εγκληματικές συμπεριφορές. Υφίσταται, ωστόσο, μια σειρά νομοθετημάτων για την κυβερνοασφάλεια,

---

[86] *Πρόταση Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τη θέσπιση εναρμονισμένων κανόνων σχετικά με την τεχνητή νοημοσύνη (Πράξη για την Τεχνητή Νοημοσύνη – AI Act) και για την τροποποίηση ορισμένων νομοθετημάτων πράξεων της Ένωσης*, Βρυξέλλες 21.04.2021, COM(2021) 206 final, 2021/0106(COD). Διαθέσιμο σε https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A52021PC0206 (Τελευταία πρόσβαση: 19.05.2023)

[87] Madiega, T., Car, P. et aI., (2022), ό.π., σελ. 7

[88] Murphy, S. et aI., (2021) 'The Metaverse: The evolution of a universal digital platform'. Διαθέσιμο σε: https://www.nortonrosefulbright.com/en-gr/knowledge/publications/5cd471a1/the-metaverse-the-evolution-of-a-universal-digital-platform (Τελευταία πρόσβαση: 11.06.2023)

[89] *Πρόταση Οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προσαρμογή των κανόνων περί εξωσυμβατικής αστικής ευθύνης στην τεχνητή νοημοσύνη (οδηγία περί ευθύνης για την ΤΝ)*, Βρυξέλλες, 28.9.2022, COM(2022) 496 final, 2022/0303(COD). Διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:52022PC0496 (Τελευταία πρόσβαση: 13.06.2023)

[90] *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).* Διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32016R0679 (Τελευταία πρόσβαση: 13.06.2023)

[91] Europol (2022), *Policing in the metaverse: what law enforcement needs to know, an observatory report from the Europol Innovation Lab*, Luxembourg: Publications Office of the European Union. Διαθέσιμο σε: https://www.europol.europa.eu/cms/sites/default/files/documents/Policing%20in%20the%20metaverse%20-%20what%20law%20enforcement%20needs%20to%20know.pdf (Τελευταία πρόσβαση: 13.06.2023), σελ. 25

όπως η νέα Οδηγία NIS 2[92], με σκοπό, μεταξύ άλλων, την εξασφάλιση ενός υψηλού επιπέδου κυβερνοασφάλειας εντός της Ε.Ε., ενώ θα μπορούσε να εφαρμοστεί και η Πρόταση Κανονισμού σχετικά με οριζόντιες απαιτήσεις κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία (EU Cyber Resilience Act - CRA), μόλις υιοθετηθεί[93].

Αξίζει να σημειωθεί ότι αναφορικά με τη χρήση της τεχνολογίας Blockchain εντός του metaverse καθώς και των NFTs θα μπορούσε να εφαρμοστεί ο νέος Κανονισμός για τις αγορές κρυπτογραφημένων περιουσιακών στοιχείων[94] καθώς και η οδηγία περί της καταπολέμησης της νομιμοποίησης εσόδων από παράνομες δραστηριότητες[95] αναφορικά με τα NFTs, τα οποία επί του παρόντος δεν ρυθμίζονται από ειδικό νομοθετικό πλαίσιο στην Ε.Ε.[96].

Επιπροσθέτως, σχετικά με τις συσκευές που χρησιμοποιούνται στο metaverse π.χ. ακουστικά εικονικής πραγματικότητας, τούτα θα μπορούσαν να υπαχθούν στην έννοια των αγαθών της Οδηγίας 2019/771 περί των συμβάσεων πώλησης αγαθών[97], η οποία εφαρμόζεται στις συμβάσεις πώλησης μεταξύ καταναλωτή και πωλητή και άρα να τύχει εφαρμογής και στο metaverse η ως άνω Οδηγία[98]. Θα μπορούσε, επίσης, να τύχει εφαρμογής

---

[92] *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).* Διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32022L2555 (Τελευταία πρόσβαση: 13.06.2023)

[93] *Πρόταση Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με οριζόντιες απαιτήσεις κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία και με την τροποποίηση του κανονισμού (ΕΕ) 2019/1020,* Βρυξέλλες, 15.9.2022, COM(2022) 454 final, 2022/0272(COD). Διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:52022PC0454 (Τελευταία πρόσβαση: 13.06.2023)

[94] *Κανονισμός (ΕΕ) 2023/1114 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 31ης Μαΐου 2023 για τις αγορές κρυπτοστοιχείων και για την τροποποίηση των κανονισμών (ΕΕ) αριθ. 1093/2010 και (ΕΕ) αριθ. 1095/2010 και των οδηγιών 2013/36/ΕΕ και (ΕΕ) 2019/1937.* Διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:32023R1114 (Τελευταία πρόσβαση: 17.06.2023)

[95] *Οδηγία (ΕΕ) 2018/843 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 30ής Μαΐου 2018, για την τροποποίηση της οδηγίας (ΕΕ) 2015/849 σχετικά με την πρόληψη της χρησιμοποίησης του χρηματοπιστωτικού συστήματος για τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες ή για τη χρηματοδότηση της τρομοκρατίας, και για την τροποποίηση των οδηγιών 2009/138/ΕΚ και 2013/36/ΕΕ (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ).* Διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32018L0843 (Τελευταία πρόσβαση: 13.06.2023)

[96] Madiega, T., Car, P. et aI., (2022), ό.π., σελ. 8

[97] *Οδηγία (ΕΕ) 2019/771 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 20ής Μαΐου 2019, σχετικά με ορισμένες πτυχές που αφορούν τις συμβάσεις για τις πωλήσεις αγαθών, την τροποποίηση του κανονισμού (ΕΕ) 2017/2394 και της οδηγίας 2009/22/ΕΚ, και την κατάργηση της οδηγίας 1999/44/ΕΚ.* Διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/el/TXT/?uri=CELEX%3A32019L0771 (Τελευταία πρόσβαση: 14.07.2023)

[98] Maciejewski, M. (2023), ό.π., σελ. 100

στο metaverse και η Οδηγία 2019/770 περί των συμβάσεων προμήθειας ψηφιακού περιεχομένου και ψηφιακών υπηρεσιών[99].

Επιπλέον, θα μπορούσε ενδεικτικά να εφαρμοστεί και η Πρόταση Κανονισμού για τη θέσπιση κανόνων με σκοπό την πρόληψη και την καταπολέμηση της σεξουαλικής κακοποίησης παιδιών[100] με στόχο την προστασία τους και σε ψηφιακά περιβάλλοντα[101]. Σημειωτέον ότι η Ευρωπαϊκή Επιτροπή ενέκρινε πρόσφατα μια νέα στρατηγική, η οποία ξεπερνά τα όρια του Web 3.0 και συμπεριλαμβάνει και το μελλοντικό Web 4.0 σε συνδυασμό με τους εικονικούς κόσμους. Η γενιά Web 4.0 είναι ικανή να συμβάλλει στην ενοποίηση των ψηφιακών αντικειμένων με τα πραγματικά αντικείμενα και περιβάλλοντα ενώ δύναται να ενδυναμώσει τις αλληλεπιδράσεις μεταξύ των ατόμων και των μηχανών. Η εν λόγω στρατηγική έχει ως σκοπό, μεταξύ άλλων, να καταστήσει τους εικονικούς κόσμους ασφαλείς και να εξασφαλίσει ότι οι εν λόγω εικονικοί κόσμοι συμβαδίζουν με τα θεμελιώδη δικαιώματα, τις αξίες και αρχές της Ευρωπαϊκής Ένωσης[102].

Σε κάθε περίπτωση, θα πρέπει οι νομοθέτες να βρίσκονται σε εγρήγορση προκειμένου να μπορούν να ανταποκριθούν στην άμεση και ορθή ρύθμιση οποιασδήποτε νέας κατάστασης προκύψει και οφείλεται στη χρήση του metaverse. Θα πρέπει ιδίως να παραμένουν σε ετοιμότητα για ανάληψη νέων πρωτοβουλιών με σκοπό την ορθή αντιμετώπιση του επικίνδυνου ή παράνομου περιεχομένου εντός του metaverse καθορίζοντας και πέρα από την ευθύνη των διαδικτυακών διαμεσολαβητών, την τυχόν ευθύνη των άβαταρ και αν τούτα αποκτούν ή όχι νομική προσωπικότητα[103].

---

[99] *Οδηγία (ΕΕ) 2019/770 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 20ής Μαΐου 2019, σχετικά με ορισμένες πτυχές που αφορούν τις συμβάσεις για την προμήθεια ψηφιακού περιεχομένου και ψηφιακών υπηρεσιών.* Διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32019L0770 (Τελευταία πρόσβαση: 14.07.2023)

[100] *Πρόταση Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τη θέσπιση κανόνων με σκοπό την πρόληψη και την καταπολέμηση της σεξουαλικής κακοποίησης παιδιών*, Βρυξέλλες, 11.5.2022, COM(2022) 209 final, 2022/0155(COD). Διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:52022PC0209 (Τελευταία πρόσβαση: 13.06.2023)

[101] Madiega, T., Car, P. et aI., (2022), ό.π., σελ. 10

[102] Ευρωπαϊκή Επιτροπή (2023), *Προς την επόμενη τεχνολογική μετάβαση: η Επιτροπή παρουσιάζει στρατηγική της ΕΕ για την ανάληψη ηγετικής θέσης στο Web 4.0 και στους εικονικούς κόσμους.* Διαθέσιμο σε: https://ec.europa.eu/commission/presscorner/detail/el/ip_23_3718 (Τελευταία πρόσβαση: 14.07.2023)

[103] Madiega, T., Car, P. et aI., (2022), ό.π., σελ. 7

3. METAVERSE ΚΑΙ ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Μια βασική πρόκληση που ανακύπτει στο πλαίσιο του metaverse είναι η επεξεργασία και προστασία των προσωπικών δεδομένων εντός του metaverse καθώς μέσω αυτού θα μπορεί να πραγματοποιείται επεξεργασία προσωπικών δεδομένων από τις πλατφόρμες με τρόπο, ώστε να υπάρχει μεγαλύτερη πληροφόρηση αναφορικά με τις σκέψεις και τη συμπεριφορά των πελατών/χρηστών τους ούτως ώστε να προσφέρεται σε αυτούς στοχευμένο περιεχόμενο[104]. Άλλωστε, η επεξεργασία βιομετρικών δεδομένων καθίσταται αναγκαία προκειμένου να παρέχεται στο χρήστη η μοναδική εμπειρία της εμβύθισης στο metaverse με τον καλύτερο δυνατό τρόπο, θέτοντας το βασικό ζήτημα της εφαρμογής και συνακολούθως συμμόρφωσης των πλατφορμών με τον GDPR[105] ιδίως με δεδομένο ότι τα βιομετρικά δεδομένα υπάγονται στις ειδικές κατηγορίες προσωπικών δεδομένων και άρα πρέπει να πληρούνται επιπρόσθετες προϋποθέσεις εξ απόψεως GDPR π.χ. ρητή συγκατάθεση για κάθε επιμέρους σκοπό.

Σημαντικός δε αλλά και ταυτόχρονα δυσχερής ανακύπτει ο καθορισμός των ρόλων και ευθυνών εξ απόψεως προσωπικών δεδομένων εντός του metaverse καθώς δεν είναι πάντοτε προφανές το ποιος καθορίζει το σκοπό της επεξεργασίας. Καθίσταται ήδη σαφές το πόσο αναγκαία είναι η λήψη μέτρων με σκοπό την προστασία των προσωπικών δεδομένων των χρηστών και δη των ανηλίκων χρηστών εντός του metaverse με δεδομένο ότι οι προκλήσεις σε επίπεδο προσωπικών δεδομένων ήδη είναι αρκετές, οι δε κίνδυνοι αυξανόμενοι.

3.1. Metaverse, GDPR και επεξεργασία προσωπικών δεδομένων

Καταρχάς, η ιδέα του metaverse έχει πραγματοποιήσει με έντονο τρόπο την εμφάνιση της στη σημερινή εποχή, στην οποία κατά μία άποψη τα προσωπικά δεδομένα είναι «*πιο πολύτιμα και από το πετρέλαιο*»[106]. Τούτο αποκτά ακόμα μεγαλύτερη σημασία λαμβάνοντας υπόψιν την άποψη σχετικά με το ότι αν δεν πληρώνει ο χρήστης για ένα προϊόν ή μια υπηρεσία στο διαδίκτυο, τότε τα δεδομένα του ίδιου του χρήστη είναι το αντίτιμο, ήτοι το ίδιο το προϊόν, μια πρακτική, την οποία ακολουθούν σήμερα ως επί το πλείστον οι περισσότερες

[104] Murphy, S. et aI., (2021), ό.π.
[105] Europol (2022), ό.π., σελ. 15
[106] Buck, L. and McDonell, R. (2022) 'Security and Privacy in the Metaverse: The Threat of the Digital Human', *CHI EA '22, April 29 - May 5, 2022,* New Orleans, LA, USA. Διαθέσιμο σε: https://www.researchgate.net/publication/360476399_Security_and_Privacy_in_the_Metaverse_The_Threat_of_the_Digital_Human (Τελευταία πρόσβαση: 13.06.2023), σελ.1

πλατφόρμες κοινωνικής δικτύωσης, οι οποίες παρέχουν «δωρεάν» τις υπηρεσίες τους, σκιαγραφώντας το πλήρες προφίλ των χρηστών και προβάλλοντας τους τις κατάλληλες διαφημίσεις[107]. Τούτο είναι σημαντικό καθώς εντός του metaverse, ιδίως στην περίπτωση που θα παρέχονται οι σχετικές υπηρεσίες δωρεάν, θα πραγματοποιείται συλλογή και επεξεργασία μιας σειράς προσωπικών δεδομένων, είτε απλών, είτε προσωπικών δεδομένων ειδικών κατηγοριών («ευαίσθητα δεδομένα»), σύμφωνα με τους αντίστοιχους ορισμούς του GDPR, ο οποίος σε μεγάλο βαθμό μπορεί να τύχει εφαρμογής και εντός του metaverse[108] προκειμένου να προστατευτούν οι χρήστες επαρκώς κατά την επεξεργασία των προσωπικών τους δεδομένων.

Ωστόσο, δεν πρέπει να λησμονείται ότι το εδαφικό πεδίο εφαρμογής του GDPR είναι συγκεκριμένο καθώς, σύμφωνα με το άρθρο 3 του Κανονισμού, ο GDPR εφαρμόζεται κυρίως «*όταν η επεξεργασία δεδομένων προσωπικού χαρακτήρα πραγματοποιείται 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*». Εφαρμόζεται, επίσης, σύμφωνα με το ως άνω άρθρο, «*στην επεξεργασία δεδομένων προσωπικού χαρακτήρα υποκειμένων των δεδομένων που βρίσκονται στην Ένωση από υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία μη εγκατεστημένο στην Ένωση, εάν οι δραστηριότητες επεξεργασίας σχετίζονται με: α) την προσφορά αγαθών ή υπηρεσιών 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*».

Επομένως, εντός του metaverse θα τεθεί εκ νέου το ζήτημα της εφαρμογής του Κανονισμού στο πλαίσιο εκτός Ε.Ε. καθώς φαίνεται πως σε ένα βαθμό η υπάρχουσα νομοθεσία για την προστασία των προσωπικών δεδομένων υστερεί σε σύγκριση με τις καινοτομίες που προσφέρονται στο metaverse. Ένα σαφές παράδειγμα συνιστά το γεγονός ότι το metaverse από τη φύση του δεν διαθέτει σύνορα και άρα είναι αβέβαιο το πώς μπορούν επί παραδείγματι να τεθούν σε εφαρμογή οι προβλέψεις περί διαβίβασης δεδομένων εκτός Ε.Ε. (Κεφάλαιο V του GDPR). Τούτο διότι από τη μία το metaverse προκειμένου να λειτουργεί ορθά, τα δεδομένα θα πρέπει να μεταβιβάζονται γρήγορα και δίχως προβλήματα, από την άλλη υφίσταται αυστηρή αντιμετώπιση των εν λόγω μεταβιβάσεων, ήτοι εκτός Ε.Ε., κάτι το

[107] Pietro, Di R., and Cresci, S. (2021), ό.π., σελ. 284
[108] Κόκιου, Β. (2022), ό.π.

οποίο διαφαίνεται και από το γεγονός ότι, σύμφωνα με την απόφαση Schrems II του Δικαστηρίου της Ευρωπαϊκής Ένωσης (ΔΕΕ), υφίσταται απαίτηση από τους εξαγωγείς δεδομένων να αξιολογούν με λεπτομερή τρόπο, το «*κατά πόσον η χώρα στην οποία διαβιβάζουν δεδομένα διαθέτει νόμους που θα της επιτρέψουν να προστατεύσει επαρκώς τα δεδομένα αυτά σύμφωνα με τα πρότυπα της Ε.Ε.*»[109].

Επίσης, κρίσιμο είναι να προσδιοριστεί αν η τοποθεσία (και όχι η χώρα καταγωγής ή ιθαγένεια) του υποκειμένου των δεδομένων που συνιστά σαφές κριτήριο για την εφαρμογή του Κανονισμού, θα προσδιοριστεί με βάση του πού εντοπίζεται ο χρήστης πίσω από το άβαταρ ή το ίδιο το άβαταρ κατά την επεξεργασία των δεδομένων του άβαταρ και ιδίως λαμβάνοντας υπόψιν ότι τα δεδομένα του τελευταίου είναι αυτά που θα τύχουν επεξεργασίας[110] ή με βάση την τοποθεσία των σχετικών διακομιστών[111]. Ωστόσο, στην περίπτωση που ως κριτήριο καθορισμού της δικαιοδοσίας, θεωρηθεί η τοποθεσία του άβαταρ, σημειώνεται ότι τούτη δεν θα μπορεί με ευκολία να προσδιοριστεί[112].

3.1.1. Σημαντικές πτυχές αναφορικά με τις κατηγορίες προσωπικών δεδομένων που συλλέγονται εντός του metaverse

Σε αντίθεση με το Web 2.0 που μέσω τούτου μπορούσαν να ανιχνευθούν πληροφορίες όπως π.χ. πού εστιάζει ο χρήστης στην οθόνη και πόση ώρα αφιερώνει ο χρήστης σε εικονιζόμενα προϊόντα και στοιχεία, στο metaverse οι εν λόγω ενέργειες συλλογής δεδομένων θα μοιάζουν παρωχημένες[113]. Παρά το γεγονός, ωστόσο, ότι, μέσω του metaverse οι δυνατότητες και το εύρος της επεξεργασίας των δεδομένων θα ξεπερνούν αυτό που συμβαίνει τη σημερινή εποχή, οι χρήστες ήδη φαίνεται να έχουν λιγότερη επίγνωση των δυνητικών κινδύνων της ιδιωτικότητας και ασφάλειάς τους σε εικονικά περιβάλλοντα σε σύγκριση με τα φυσικά[114]. Σημειωτέον ότι η είσοδος του χρήστη στο metaverse, όπως θα γινόταν αντίστοιχα με την είσοδο σε έναν ιστότοπο, οδηγεί στη συλλογή προσωπικών

---

[109] Murphy, S. et al., (2021), ό.π.

[110] Cheong, B.C. (2022) 'Avatars in the metaverse: potential legal issues and remedies'. *Int. Cybersecur. Law Rev.* **3**, 467–494. Διαθέσιμο σε: https://link.springer.com/article/10.1365/s43439-022-00056-9#citeas (Τελευταία πρόσβαση: 13.06.2023), σελ. 491

[111] Madiega, T., Car, P. et al., (2022), ό.π., σελ. 5

[112] Dwivedi, K. Y. et al. (2022), ό.π., σελ. 10

[113] Pietro, Di R., and Cresci, S. (2021), ό.π., σελ. 284

[114] Nair, V., Garido, M. G. and Song, D. (2022), *Going Incognito in the Metaverse.* Διαθέσιμο σε: https://arxiv.org/abs/2208.05604 (Τελευταία πρόσβαση: 13.06.2023), σελ.1

δεδομένων, η οποία, ωστόσο διαφοροποιείται ως προς το είδος και των όγκο των προσωπικών δεδομένων, συγκριτικά με τους ιστοτόπους[115]. Άλλωστε προκειμένου να λειτουργήσουν τα ψηφιακά περιβάλλοντα είναι αναγκαία ως επί το πλείστον η μαζική επεξεργασία προσωπικών δεδομένων των χρηστών[116]. Τρεις θεωρούνται ως οι πιο σημαντικοί τομείς σχετικά με την ιδιωτικότητα των χρηστών εντός του metaverse, ήτοι πληθώρα προσωπικών πληροφοριών αναφορικά με τις συνήθειες τους, τη συμπεριφορά τους και την επικοινωνία εν γένει[117].

Αξίζει να σημειωθεί ότι, πέραν των δεδομένων που θα εισάγει ένας χρήστης αυτοβούλως εντός της ίδιας της πλατφόρμας όπως ενδεικτικά ονοματεπώνυμο, ηλικία, στοιχεία επικοινωνίας[118], το metaverse θα μπορεί να λάβει πρόσθετες πληροφορίες όπως τις κινήσεις του σώματός, τις αντιδράσεις, τις αλληλεπιδράσεις (τόσο τις εικονικές όσο και τις ρεαλιστικές) με το περιβάλλον, «*τα εγκεφαλικά κύματα*»[119] καθώς και δυνητικά άλλα δεδομένα όπως τη διεύθυνση IP[120]. Προκειμένου, επομένως, να υφίσταται διασφάλιση μιας υψηλού επιπέδου προστασίας των υποκειμένων των δεδομένων καθίσταται αναγκαίο να συμπεριληφθούν στην έννοια των προσωπικών δεδομένων και πληροφορίες που εμμέσως αφορούν στο χρήστη π.χ. δεδομένα που τυγχάνουν συλλογής μέσω του εξοπλισμού εμβύθισης εντός του metaverse, τα οποία συνδράμουν, ενδεικτικά στο να αξιολογηθεί ο χρήστης σε διάφορους τομείς, όπως οικογενειακή κατάσταση και οικονομική θέση. Σημειωτέον ότι οι υπηρεσίες γεωεντοπισμού, οι οποίες θα λαμβάνουν χώρα στα περιβάλλοντα επαυξημένης και εικονικής πραγματικότητας μπορούν να συμβάλλουν στον εντοπισμό των προτιμήσεων των χρηστών, οι οποίες με τη σειρά τους μπορούν να οδηγήσουν στην κατάρτιση προφίλ[121].

Επομένως, πέρα από δεδομένα, τα οποία οδηγούν στην άμεση ταυτοποίηση του χρήστη, θα υφίσταται εντός του metaverse επεξεργασία προσωπικών δεδομένων, η οποία θα οδηγεί σε αποκάλυψη ειδικότερων πληροφοριών για το χρήστη. Στην πραγματικότητα, οι συσκευές τεχνολογίας XR προκειμένου να εισάγουν το χρήστη στο περιβάλλον του metaverse και προκειμένου το εν λόγω περιβάλλον να λειτουργεί με ορθό τρόπο συλλέγουν,

---

[115] Κόκιου, Β. (2022), ό.π.
[116] Καρδαμάκη, Α. (2022), ό.π., σελ. 10
[117] Pietro, Di R., and Cresci, S. (2021), ό.π., σελ. 284
[118] Καρδαμάκη, Α. (2022), ό.π., σελ. 10
[119] Pietro, Di R., and Cresci, S. (2021), ό.π., σελ. 284
[120] Καρδαμάκη, Α. (2022), ό.π., σελ. 10
[121] Καρδαμάκη, Α. (2022), ό.π., σελ. 11- 12

όπως προειπώθηκε, πολύ σημαντικό αριθμό βιομετρικών δεδομένων[122]. Δεν πρέπει να λησμονείται σε καμία περίπτωση το γεγονός πως τέτοιου είδους συλλογή προσωπικών δεδομένων, όπως παρακολούθηση του βλέμματος των ματιών που δύναται να παρέχει δεδομένα διαστολής της κόρης του ματιού καθώς και η κίνηση χεριών και σώματος που παρέχουν ενδείξεις της γλώσσας του σώματος[123] συνιστούν ειδικές κατηγορίες προσωπικών δεδομένων (βιομετρικά δεδομένα εν προκειμένω), οι οποίες οδηγούν σε πλήρη ταυτοποίηση των χρηστών[124] και οι οποίες απαιτούν ιδιαίτερη προσοχή κατά την επεξεργασία. Ενδεικτικά αξίζει να αναφερθεί ότι, σύμφωνα με μια μελέτη, «*πέντε λεπτά δεδομένων παρακολούθησης κίνησης που συλλέγονται απλώς από μια head-mounted display συσκευή κατά τη διάρκεια μιας τυπικής εργασίας προβολής αρκούν για να επέλθει ταυτοποίηση ενός χρήστη με ακρίβεια 95%*»[125], αναδεικνύοντας το πόσο απλά και γρήγορα μπορεί να υπάρξει άμεση ταυτοποίηση ενός χρήστη μέσω των εν λόγω συσκευών που θα συνδέουν το χρήστη με το περιβάλλον του metaverse.

Περαιτέρω, δεδομένα που ενδεικτικά μπορούν να συλλεχθούν από τους χρήστες τεχνολογιών VR είναι δεδομένα σχετικά με τον χρήστη π.χ. φυσική κατάσταση, συμπεριφορά, απόσταση μεταξύ των οφθαλμών, ικανότητα χειρισμού, χρόνος αντίδρασης, εν γένει οι κινήσεις του σώματος, δεδομένα σχετικά με το περιβάλλον π.χ. μέγεθος δωματίου, γεωγραφικός εντοπισμός, τεχνικά δεδομένα π.χ. μοντέλο συσκευής και δημογραφικά στοιχεία, όπως φύλο, ηλικία, εθνικότητα, εισόδημα[126] καθώς και δεδομένα για το σπίτι και την οικογένειά του[127]. Ιδιαίτερο ενδιαφέρον αποκτά το γεγονός ότι ακόμα και μία εκ των ως άνω ενεργειών δύναται να αποκαλύψει σειρά προσωπικών πληροφοριών όπως π.χ. οι προδιαγραφές της συσκευής που χρησιμοποιείται μπορεί εμμέσως να οδηγήσει στην ανίχνευση της πληροφορίας περί του εισοδήματος και της οικονομικής κατάστασης του χρήστη[128].

---

[122] Σύμφωνα με το άρθρο 4 στ'14 του GDPR, ως «βιομετρικά δεδομένα ορίζονται *τα δεδομένα προσωπικού χαρακτήρα τα οποία 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*».

[123] Buck, L. and McDonell, R. (2022), ό.π., σελ. 2

[124] Warin, C. and Reinhardt, D. (2022), ό.π., σελ. 113

[125] Buck, L. and McDonell, R. (2022), ό.π., σελ.1

[126] Nair, V., Garido, M. G. and Song, D. (2022), *Going Incognito in the Metaverse.* ό.π., σελ. 2

[127] Cheong, B.C. (2022), ό.π., σελ. 491

[128] Nair, V., Garido, M. G. and Song, D. (2022), *Exploring the Unprecedented Privacy Risks of the Metaverse.* Διαθέσιμο σε: https://arxiv.org/abs/2207.13176 (Τελευταία πρόσβαση: 14.06.2023), σελ. 3

Η δε παρακολούθηση της κίνησης ενός χρήστη δύναται να οδηγήσει σε αποκάλυψη πληροφοριών σχετικά με την υγεία ενός χρήστη, ήτοι ψυχική και σωματική κατάσταση αυτού ενώ η παρακολούθηση της αναπαράστασης του προσωπικού περιβάλλοντος του χρήστη δύναται να αποκαλύψει, είτε κοινωνικές προτιμήσεις, είτε κάποιου είδους διαταραχές, όπως το κοινωνικό άγχος, ΔΕΠΥ[129]. Άλλωστε, τα βιομετρικά δεδομένα εν γένει, όπως η παρακολούθηση του βλέμματος καθώς και ο καρδιακός ρυθμός αναδεικνύουν καίριες πτυχές του ψυχισμού του εκάστοτε χρήστη[130]. Η παρακολούθηση δε του προσώπου μπορεί να παρέχει πληροφορίες σχετικά με τη συναισθηματική απόκριση του χρήστη[131].

3.2. Προκλήσεις του metaverse στο πλαίσιο των προσωπικών δεδομένων

Πέραν της ευρείας συλλογής προσωπικών δεδομένων που λαμβάνει χώρα σε εικονικά περιβάλλοντα, όπως το metaverse τίθενται και μερικές ακόμα προκλήσεις, οι βασικές εκ των οποίων αναλύονται κατωτέρω ενδεικτικά. Καταρχάς, είναι πολύ κρίσιμος ο καθορισμός των ρόλων εξ απόψεως των προσωπικών δεδομένων εντός του metaverse, ήτοι ποιος θα αναλάβει το ρόλο του υπευθύνου, ποιος το ρόλο του εκτελούντος την επεξεργασία. Ωστόσο, σε περιβάλλοντα όπως το metaverse όπου υφίστανται διάφορες οντότητες καθίσταται δύσκολος ο προσδιορισμός των ρόλων και συνεπώς των υποχρεώσεων και ευθυνών μεταξύ τους. Ανακύπτει, επομένως, το συμπέρασμα ότι θα είναι αρκετά δυσχερής η διάκριση μεταξύ των ρόλων του υπευθύνου και του εκτελούντος την επεξεργασία εντός του metaverse λόγω του γεγονότος ότι οι εμπλεκόμενες οντότητες εντός του metaverse ενδεχομένως θα συγχέονται σε μεγάλο βαθμό και επομένως δεν θα είναι ξεκάθαρο του ποιος θα καθορίζει το σκοπό της επεξεργασίας και άρα θα είναι ο υπεύθυνος και αντίστοιχα του ποιος θα δρα για λογαριασμό του υπευθύνου και άρα θα είναι εκτελών την επεξεργασία[132] ή αν θα υφίστανται ανά περίπτωση περισσότεροι υπεύθυνοι επεξεργασίας. Κρίσιμο είναι σε κάθε περίπτωση, είτε πρόκειται για οντότητα που συνιστά υπεύθυνο επεξεργασίας, είτε οντότητα που συνιστά εκτελών την επεξεργασία, να υφίσταται διασφάλιση της προστασίας των προσωπικών δεδομένων των υποκειμένων, εξασφαλίζοντας αντιστοίχως τα δικαιώματά τους με δεδομένο ότι η επεξεργασία των

[129] Buck, L. and McDonell, R. (2022), ό.π., σελ.1
[130] Fernandez, C.B and Hui, P. (2022), ό.π., σελ. 272
[131] Buck, L. and McDonell, R. (2022), ό.π., σελ.2
[132] Madiega, T., Car, P. et aI., (2022), ό.π., σελ. 5

δεδομένων εντός του metaverse δεν θα πραγματοποιείται μόνο για ψυχαγωγικούς σκοπούς αλλά και για άλλους π.χ. στον τομέα της εργασίας[133].

Αναφορικά με τον εν γένει καθορισμό των ρόλων των εμπλεκόμενων φορέων πέραν των παρόχων της εκάστοτε πλατφόρμας, ήτοι των οντοτήτων στις οποίες ανήκει και διαχειρίζονται μια πλατφόρμα, και των χρηστών εντοπίζονται και οι στοχεύοντες φορείς[134], ήτοι χρήστες, οι οποίοι με τη συνδρομή συγκεκριμένων μηχανισμών στοχεύουν άλλους χρήστες προκειμένου να προάγουν συγκεκριμένα συμφέροντα π.χ. εμπορική προώθηση, ήτοι σαν να είναι διαφημιστές εντός του metaverse. Οι εν λόγω στοχεύοντες φορείς συνιστούν από κοινού υπεύθυνους επεξεργασίας μαζί με τους παρόχους καθώς αμφότεροι θα επεξεργάζονται τόσο τα προσωπικά δεδομένα, τα οποία εισάγονται αυτοβούλως από το χρήστη όσο και τα δεδομένα που εμμέσως αφορούν στο χρήστη ενώ η εν λόγω ιδιότητά τους ως από κοινού υπεύθυνοι επεξεργασίας ισχύει «*στην έκταση που συγκαθορίζουν τον σκοπό και τον τρόπο της επεξεργασίας*» [135].

Επίσης, ένα άλλο κύριο ζήτημα συνιστά η συγκατάθεση των χρηστών εντός του metaverse και αντιστοίχως της υποχρεωτικής ενημέρωσής τους μέσω σχετικών ειδοποιήσεων περί προστασίας της ιδιωτικότητάς τους. Ειδικότερα, τίθεται το ζήτημα του κατά πόσον οι εν λόγω πράξεις, ενημέρωση και συγκατάθεση, θα πρέπει να διενεργούνται εν γένει με την είσοδο στο metaverse συνολικά ή σε κάθε επιμέρους metaverse ξεχωριστά π.χ. ξεχωριστή συγκατάθεση για το metaverse συναυλίας και ξεχωριστή για ένα metaverse δημοπρασίας. Σύμφωνα με τις προβλέψεις του GDPR, το υποκείμενο των δεδομένων πρέπει να παρέχει τη ρητή συγκατάθεση για κάθε συγκεκριμένο και ξεχωριστό σκοπό. Ωστόσο, το metaverse από τη φύση του, συλλέγει διαρκώς προσωπικά δεδομένα, όπως αναφέρθηκε παραπάνω προκειμένου να παρέχει τα προϊόντα και υπηρεσίες του, χωρίς πολλές φορές τούτο να γίνεται αντιληπτό από τους χρήστες και άρα καθιστώντας πρακτικά δυσχερές το να λαμβάνεται διαρκώς σε όλες τις πράξεις επεξεργασίας η συγκατάθεση του χρήστη[136].

Στο σημείο αυτό, τίθεται το ζήτημα της πρακτικής εφαρμογής του GDPR, με δεδομένο ότι από τη μία θα υφίσταται κατά κόρον επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων και δη βιομετρικών δεδομένων και άρα οι πλατφόρμες θα πρέπει να είναι διαρκώς σε επαγρύπνηση προκειμένου να λαμβάνεται η συγκατάθεση των υποκειμένων

[133] Καρδαμάκη, Α. (2022), ό.π., σελ. 13
[134] Καρδαμάκη, Α. (2022), ό.π., σελ. 14
[135] Καρδαμάκη, Α. (2022), ό.π., σελ. 15-16
[136] Madiega, T., Car, P. et aI., (2022), σελ. 5

των δεδομένων, πρακτικά δυσχερές όπως αναφέρεται ανωτέρω, από την άλλη ενδέχεται η υπερβολική προσπάθεια συμμόρφωσης με τον GDPR να φέρει τα αντίθετα αποτελέσματα από εκείνα που στοχεύει ο GDPR π.χ. αδυναμία χρηστών να κατανοήσουν τυχόν δυσνόητους και πολλαπλούς όρους χρήσης[137].

Περαιτέρω, τίθεται το ζήτημα της νόμιμης βάσης επεξεργασίας εντός του metaverse, το οποίο θα συλλέγει τόσο απλές κατηγορίες όσο και ειδικές κατηγορίες προσωπικών δεδομένων. Εν γένει κατά την επεξεργασία απλών δεδομένων, πέραν της συγκατάθεσης, όπως αναφέρθηκε ανωτέρω, η σύμβαση (άρθρο 6 στοιχ. β' GDPR) παρουσιάζεται καταρχήν ως η κατάλληλη νόμιμη βάση επεξεργασίας για την εκτέλεση της σύμβασης παροχής επιγραμμικών υπηρεσιών στην οποία το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή με σκοπό τη λήψη μέτρων με αίτηση του υποκειμένου των δεδομένων κατά το προσυμβατικό στάδιο. Τούτο, ωστόσο, δεν σημαίνει ότι κάθε άλλη υπηρεσία π.χ. βελτίωση υπηρεσιών, επεξεργασία για διαφημιστικούς λόγους που παρέχεται εξ αφορμής της αρχικής σύμβασης κρίνεται αναγκαία για τους σκοπούς της εν λόγω σύμβασης (εκτέλεσης σύμβασης στο πλαίσιο παροχής επιγραμμικών υπηρεσιών) και άρα ενδέχεται να απαιτείται η εύρεση νέας νόμιμης βάσης επεξεργασίας. Ενδεικτικά επομένως, η επεξεργασία που διενεργείται για διαφημιστικό σκοπό θα πρέπει να καλύπτεται από τη δική της νόμιμη βάση καθώς ο χρήστης δεν συμβάλλεται συνήθως σε συμβάσεις, όπως η ανωτέρω, με σκοπό την κατάρτιση προφίλ και άρα δεν υφίσταται νόμιμη βάση επεξεργασίας για τους διαφημιστικούς σκοπούς αλλά ο χρήστης συμβάλλεται κατά κανόνα προκειμένου να του παρασχεθούν οι εκάστοτε σχετικές υπηρεσίες (παροχή επιγραμμικών υπηρεσιών)[138].

Σε αντίθεση με τα παραπάνω, η επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων καταρχήν απαγορεύεται σύμφωνα με τις προβλέψεις του άρθρου 9 του GDPR. Η επεξεργασία ειδικών κατηγοριών δεδομένων επιτρέπεται μόνο υπό συγκεκριμένες περιπτώσεις, στις οποίες δεν περιλαμβάνεται η εκτέλεση της σύμβασης ως νόμιμη βάση επεξεργασίας. Επομένως, πέραν της συγκατάθεσης του υποκειμένου των δεδομένων, η οποία πρέπει να είναι ελεύθερη, ρητή, συγκεκριμένη και εν πλήρει επιγνώσει[139], θα πρέπει να αναζητηθεί μια άλλη νόμιμη βάση επεξεργασίας, η οποία να καλύπτει την επεξεργασία βιομετρικών δεδομένων, τα οποία χρησιμοποιούνται για την εμβύθιση του χρήστη, κάτι το

[137] Καρδαμάκη, Α. (2022), ό.π., σελ. 21
[138] Καρδαμάκη, Α. (2022), ό.π., σελ. 17
[139] Σύμφωνα με το άρθρο 4 σημείο 11) του GDPR.

οποίο όμως αποδεικνύεται δυσχερές καθώς οι λοιπές νόμιμες βάσεις επεξεργασίας δεν φαίνεται να συνάδουν σε περιβάλλοντα, όπως το metaverse και για την παροχή των σχετικών υπηρεσιών[140], ούτως ώστε η συγκατάθεση να μοιάζει μονόδρομος εν προκειμένω.

Τέλος, η δυνατότητα διαλειτουργικότητας σε συνδυασμό με την τυχόν μετακίνηση των χρηστών εντός διαφορετικών metaverses διατηρώντας τα δεδομένα και τα περιουσιακά τους στοιχεία δημιουργεί το ζήτημα της κοινής χρήσης και φορητότητας των δεδομένων. Σύμφωνα με την υπ'αριθμ. 68 αιτιολογική σκέψη του GDPR, «*οι εταιρείες, οι οποίες τείνουν να προτιμούν τα ιδιοκτησιακά δικαιώματα επί των δεδομένων των χρηστών, θα πρέπει να καταρτίσουν συμφωνίες ανταλλαγής δεδομένων, οι οποίες θα πρέπει να πληρούν τις απαιτήσεις προστασίας των δεδομένων, όπως η συγκατάθεση των χρηστών και η υποχρέωση κοινοποίησης της ιδιωτικής ζωής*». Η εν λόγω πρόβλεψη μπορεί να θέσει νέες προκλήσεις κατά τη φορητότητα δεδομένων σε αποκεντρωμένα μοντέλα metaverse ενώ κατά την κοινή χρήση των δεδομένων με τρίτα μέρη θα απαιτεί εκ νέου τη συγκατάθεση του υποκειμένου των δεδομένων, μια εμφανή πρόκληση εξ αφορμής του metaverse, «*στο οποίο οι χρήστες μπορεί να υπόκεινται όλο και περισσότερο σε υποσυνείδητη διαφήμιση*»[141].

Συνεπώς, καθίσταται σαφές ότι προκειμένου να ικανοποιείται η διαλειτουργικότητα στο metaverse θα πρέπει μεν να επιτρέπεται η φορητότητα και η κοινή χρήση των δεδομένων από τους φορείς εκμετάλλευσης, έτσι ώστε οι χρήστες να έχουν τη δυνατότητα εναλλαγής μεταξύ των επιμέρους πλατφορμών του metaverse δίχως όμως να παραβλέπονται οι κίνδυνοι που απορρέουν από τη φορητότητα των δεδομένων μέσω της οποίας εντός του metaverse θα μεταφέρεται μεγάλη ποσότητα προσωπικών δεδομένων[142]. Ούτως ή άλλως η δυνατότητα φορητότητας των δεδομένων, κατ' εφαρμογή του GDPR, αντιμετωπίζει, επί του παρόντος, τεχνικές και πρακτικές δυσκολίες καθώς διενεργείται, μεταξύ άλλων, στην περίπτωση που τα προσωπικά δεδομένα τυγχάνουν επεξεργασίας με αυτοματοποιημένα μέσα[143].

---

[140] Καρδαμάκη, Α. (2022), ό.π., σελ. 18

[141] Madiega, T., Car, P. et al., (2022), ό.π., σελ. 5

[142] Arzt, M. and Weingarden, G. (2022), 'Metaverse and privacy'. Διαθέσιμο σε: https://iapp.org/news/a/metaverse-and-privacy-2/ (Τελευταία πρόσβαση: 14.06.2023)

[143] Σύμφωνα με το άρθρο 20 παρ. 1β του GDPR.

3.3. Κίνδυνοι από τη χρήση δεδομένων εντός του metaverse

Εκτός από τις σημαντικές προκλήσεις που δημιουργεί το metaverse, θέτει και μια σειρά από υπαρκτούς κινδύνους εις βάρος των χρηστών. Καταρχάς, λαμβάνοντας υπόψιν ότι το metaverse θα περιέχει αλγορίθμους, οι οποίοι θα τροφοδοτούνται από βιομετρικά δεδομένα μπορεί τούτο να ενισχύσει και να επιδεινώσει τα φαινόμενα ανισοτήτων σε διάφορα κοινωνικά περιβάλλοντα αποκαλύπτοντας ευαίσθητες πληροφορίες για το χρήστη π.χ. υπάρχουσα αναπηρία, σεξουαλικές προτιμήσεις του χρήστη απλώς και μόνο μέσω των δεδομένων βλέμματος[144]. Άλλωστε είναι γνωστό ότι οι κοινωνικές ανισότητες επέρχονται σε πολλές περιπτώσεις μεροληπτικών μοντέλων Big Data, τα οποία επεξεργάζονται μια σειρά ειδικών κατηγοριών προσωπικών δεδομένων καταλήγοντας σε κοινωνικό αποκλεισμό και διακρίσεις π.χ. εις βάρος των γυναικών, των έγχρωμων ατόμων κ.λπ.[145].

Κάτι αντίστοιχο θα μπορούσε να πραγματοποιηθεί και σε εργασιακούς χώρους του metaverse, όπου λαμβάνοντας υπόψιν τα προσωπικά δεδομένα των χρηστών εργαζομένων, τα οποία δεν εισάγονται πάντοτε αυτοβούλως από τους χρήστες εργαζομένους, οι εργοδότες θα μπορούσαν παράνομα και παρεμβατικά να επιτηρούν τους εργαζομένους τους ενώ θα μπορούσε να λάβει χώρα και μεροληπτική αυτοματοποιημένη λήψη αποφάσεων και δημιουργία ανισοτήτων γενικά π.χ. κατά την πρόσληψη, κατά την αξιολόγηση της απόδοσης του χρήστη κ.λπ.[146].

Επιπλέον, εν γένει υφίστανται κίνδυνοι και ανησυχίες στο περιβάλλον του metaverse στο πλαίσιο της ιδιωτικότητας και ασφάλειας λόγω της φύσης των ίδιων των υφιστάμενων τεχνολογιών του π.χ. XR, blockchain καθώς ναι μεν εφαρμόζονται ορισμένα χαρακτηριστικά ασφαλείας αλλά απουσιάζουν ουσιώδη μέτρα προστασίας της ιδιωτικότητας[147]. Ως εκ τούτου, υφίσταται το πρόσφορο έδαφος που δημιουργεί εμφανή τον κίνδυνο διαρροής δεδομένων σε τρίτους και παραβίασης της ιδιωτικότητας καθώς και ασφάλειας των προσωπικών δεδομένων, εξαιτίας του μεγάλου όγκου δεδομένων που τυγχάνουν συλλογής και επεξεργασίας από τους ενσωματωμένους αισθητήρες που διαθέτουν οι συσκευές XR[148].

Επιπροσθέτως, ένας ακόμη κίνδυνος που δημιουργείται εξ αφορμής των συσκευών XR προέρχεται από τα χωρικά δεδομένα (συμπεριλαμβανομένου του φυσικού

[144] Fernandez, C.B and Hui, P. (2022), ό.π., σελ. 273
[145] Warin, C. and Reinhardt, D. (2022), ό.π., σελ.112
[146] Madiega, T., Car, P. et aI., (2022), ό.π., σελ. 5
[147] Warin, C. and Reinhardt, D. (2022), ό.π., σελ. 112
[148] Warin, C. and Reinhardt, D. (2022), ό.π., σελ. 113

περιβάλλοντος του χρήστη), τα οποία κρίνονται απαραίτητα προκειμένου η συσκευή να λειτουργεί ορθά ενώ έχει αποδειχθεί ότι υφίσταται ο κίνδυνος της ταυτοποίησης του χώρου του χρήστη, χωρίς τούτος να γνωρίζει με βεβαιότητα ότι οι εν λόγω συσκευές ή συναφείς συσκευές, όπως ενσωματωμένες κάμερες προβαίνουν σε καταγραφή τέτοιου είδους υλικού[149]. Οι συσκευές XR, επομένως, μπορεί ναι μεν να επιτρέπουν μια βελτιωμένη και ρεαλιστική εμπειρία στο metaverse αλλά ταυτόχρονα δημιουργούν μια σειρά κινδύνων για την προστασία της ιδιωτικότητας τόσο του χρήστη όσο και των παρευρισκομένων στο φυσικό περιβάλλον του χρήστη με δεδομένο ότι μπορούν να τύχουν επεξεργασίας και δεδομένα των παρευρισκόμενων ατόμων.

Περαιτέρω, εντός του metaverse υφίσταται μια σειρά από κινδύνους εις βάρος των προσωπικών δεδομένων ευάλωτων ομάδων, όπως παιδιών, τα οποία σύμφωνα με τον GDPR πρέπει να τυγχάνουν ειδικής προστασίας. Τα παιδιά δύνανται να εκτεθούν σε κινδύνους, όπως ενδεικτικά η παιδική πορνογραφία, πρόσβαση σε ακατάλληλο και ενδεχομένως βίαιο υλικό και περιεχόμενο για την ηλικία τους[150], όπως ενδελεχώς θα αναφερθεί και στο πέμπτο κεφάλαιο της παρούσας, καθώς και να παρέχουν μια σειρά προσωπικών δεδομένων ειδικών κατηγοριών και τούτα να διαρρεύσουν σε τρίτους.

Τέλος, η εν γένει πρόσβαση και επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων δύναται να οδηγήσει σε παράνομους τρόπους κατάρτισης προφίλ με δυσμενείς συνέπειες για το υποκείμενο των δεδομένων, όπως επί παραδείγματι απώλεια του ελέγχου των αποφάσεών του ή ανά περίπτωση επιρροή αποφάσεων ευάλωτων κοινωνικών ομάδων, οι οποίες δυνητικά σε εκλογική διαδικασία θα μπορούσαν να χειραγωγηθούν με αποτέλεσμα την αύξηση της κρατικής εποπτείας λαμβάνοντας υπόψιν ότι δυνητικά υφίσταται πρόσβαση των κυβερνητικών οργάνων στα δεδομένα εντός του metaverse. Σημειωτέον ότι μέσω της ιχνηλάτισης βλέμματος (χρήση eye-trackers), εμφανής είναι και ο κίνδυνος της στοχευμένης διαφήμισης εκ μέρους των εταιρειών σε εξαιρετικά διεξοδικό επίπεδο[151].

[149] Warin, C. and Reinhardt, D. (2022), ό.π., σελ.112
[150] Κόκιου, Β. (2022), ό.π.
[151] Madiega, T., Car, P. et aI., (2022), ό.π., σελ. 5

3.4. Προτάσεις για την προστασία της ιδιωτικότητας εντός του metaverse

Καταρχάς, όλες οι πολιτικές και πρακτικές εκ μέρους των εταιρειών οφείλουν να είναι κατανοητές, διαφανείς και εύκολα προσβάσιμες από όλους τους χρήστες του metaverse. Ως εκ τούτου, όλοι οι εμπλεκόμενοι φορείς στη δημιουργία και διαχείριση του metaverse οφείλουν να λαμβάνουν τα κατάλληλα μέτρα, τεχνικά και οργανωτικά καθώς και διαφανείς πολιτικές προκειμένου να συμμορφώνονται τόσο με την ισχύουσα νομοθεσία περί προσωπικών δεδομένων όσο και να επιτύχουν την εξασφάλιση της εμπιστοσύνης των χρηστών[152].

Ειδικότερα, ορθή πρακτική εκ μέρους των εταιρειών θα ήταν να βρίσκεται στο επίκεντρο ο χρήστης και η προστασία του, επομένως θα μπορούσαν να υφίστανται συγκεκριμένα βήματα υπέρ της προστασίας του χρήστη π.χ. κατά τη χρήση συσκευών XR. Πιο συγκεκριμένα, θα μπορούσε αρχικά ο χρήστης να εγκαταστήσει και να εγγραφεί σε συγκεκριμένη εφαρμογή, μέσω της οποίας θα εισέρχεται στο περιβάλλον του metaverse κάνοντας χρήση της συσκευής XR, αλλά προηγουμένως θα πρέπει να έχει αποδεχτεί τις πολιτικές απορρήτου, οι οποίες θα περιέχουν προβλέψεις για διαφανή συλλογή προσωπικών δεδομένων. Περαιτέρω θα πρέπει ο χρήστης να μπορεί να έχει εύκολα πρόσβαση σε όσα προσωπικά δεδομένα συλλέγονται για λογαριασμό του σε περιβάλλοντα του metaverse ενώ κάθε φορά που θα δίνεται η δυνατότητα να έχουν τρίτοι πρόσβαση σε προσωπικά δεδομένα του χρήστη, αυτός θα πρέπει προηγουμένως να προεγκρίνει την εν λόγω πρόσβαση. Σε κάθε περίπτωση, θα πρέπει οι φορείς να διασφαλίζουν την ασφαλή αλληλεπίδραση μεταξύ των χρηστών ενώ θα πρέπει ο χρήστης να διατηρεί τη δυνατότητα ανάκλησης των τυχόν χορηγούμενων δικαιωμάτων πρόσβασης και φυσικά να μπορεί ανά πάσα στιγμή να απεγκαταστήσει την εν λόγω εφαρμογή[153].

Κρίσιμη είναι και η προστασία των προσωπικών δεδομένων των παιδιών εντός του metaverse, τα οποία, όπως αναφέρθηκε ανωτέρω, διατρέχουν υψηλούς κινδύνους. Ως εκ τούτου, υφίσταται η απαίτηση ήδη από τον GDPR, για ιδιαίτερη προστασία των προσωπικών δεδομένων των παιδιών ενώ οι αρχές προστασίας δεδομένων προσωπικού χαρακτήρα σε περιπτώσεις που υφίσταται επεξεργασία προσωπικών δεδομένων ανηλίκων είναι αμείλικτες με οργανισμούς που δεν τηρούν και δεν εφαρμόζουν ιδιαίτερη προστατευτική

[152] Fernandez, C.B and Hui, P. (2022), ό.π., σελ. 274
[153] Warin, C. and Reinhardt, D. (2022), ό.π., σελ.114

μεταχείριση των δεδομένων των ανηλίκων[154]. Στο εν λόγω πλαίσιο, θα πρέπει να υφίσταται επαλήθευση της ηλικίας των ανηλίκων προτού τούτα συνδεθούν σε περιβάλλοντα του metaverse και προκειμένου να αποφευχθεί η παροχή προσωπικών δεδομένων εκ μέρους τους[155].

Ειδικότερα, η επαλήθευση της ηλικίας ή η ύπαρξη συγκεκριμένων περιορισμών λόγω της ηλικίας σε συγκεκριμένους χώρους του metaverse θα πρέπει να διενεργείται μέσω εξελιγμένων τεχνικών ενώ αδήριτη είναι και η ανάγκη για ουσιαστική εφαρμογή μέτρων, τα οποία θα αποθαρρύνουν καταρχήν τους ανηλίκους από το να εισάγουν προσωπικά δεδομένα τους εντός του metaverse και θα συμβάλλουν στην αδιάκοπη και σταθερή προσπάθεια του συνόλου των εμπλεκόμενων μερών υπέρ της ασφάλειας των ανηλίκων σε ψηφιακά περιβάλλοντα[156]. Αξίζει να σημειωθεί ότι αναφορικά με το ζήτημα της συγκατάθεσης κατά την προσφορά υπηρεσιών της κοινωνίας των πληροφοριών κατευθείαν σε ανήλικο, σύμφωνα με το άρθρο 21 του ελληνικού εφαρμοστικού νόμου 4624/2019, η επεξεργασία είναι σύννομη εφόσον ο ανήλικος έχει συμπληρώσει το 15ο έτος της ηλικίας του και παρέχει τη συγκατάθεσή του. Σε διαφορετική περίπτωση (ηλικία ανηλίκου κάτω των 15 ετών), η επεξεργασία είναι νόμιμη μόνο εφόσον παρέχει τη συγκατάθεση του ο νόμιμος αντιπρόσωπος του ανηλίκου, κάτι το οποίο, κατόπιν εύλογων προσπαθειών του υπευθύνου επεξεργασίας, και με δεδομένη τη διαθέσιμη τεχνολογία, σύμφωνα με το άρθρο 8 παρ. 2 του GDPR θα μπορεί να τύχει επαλήθευσης περί του αν η συγκατάθεση έχει ληφθεί από το πρόσωπο που διαθέτει τη γονική μέριμνα του ανηλίκου.

Σε κάθε περίπτωση επεξεργασίας προσωπικών δεδομένων, είτε χρηστών ανηλίκων είτε χρηστών ενηλίκων, καθίσταται αναγκαία η αύξηση της ευαισθητοποίησης των χρηστών αναφορικά με την παραβίαση και διαρροή δεδομένων προκειμένου οι χρήστες να είναι ουσιαστικά ενήμεροι για το τι προσωπικά δεδομένα μοιράζονται εντός του metaverse και παρέχοντας τους την ευκαιρία να είναι πιο προσεχτικοί επιλέγοντας ενίοτε να μην αποκαλύπτουν προσωπικά δεδομένα τους και αποθαρρύνοντας με αυτό τον τρόπο τις οιεσδήποτε επιθέσεις εις βάρος των δεδομένων τους[157].

Κρίνεται δε αναγκαίος ο προσδιορισμός των ρόλων των φορέων και στο πλαίσιο των δυνητικών κινδύνων ως προς τα δεδομένα των χρηστών προκειμένου να καθοριστεί η

[154] Murphy, S. et aI., (2021), ό.π.
[155] Madiega, T., Car, P. et aI., (2022), ό.π., σελ. 5
[156] Κόκιου, Β. (2022), ό.π.
[157] Warin, C. and Reinhardt, D. (2022), ό.π., σελ.113

ευθύνη καθενός και να διασφαλίζει το κάθε μέρος στην έκταση που του αναλογεί και εφόσον δεν υφίστανται τεχνικές δυσκολίες και περιορισμοί, την άσκηση των δικαιωμάτων των χρηστών αναφορικά με την προστασία των προσωπικών τους δεδομένων. Σε κάθε δε περίπτωση είναι αναγκαία η ύπαρξη σύμβασης (ΣΕΔ) ή άλλης νομικής πράξης μεταξύ του υπευθύνου και του εκτελούντος την επεξεργασία, όπως προβλέπεται στο άρθρο 28 παρ. 3 του GDPR και η οποία πρέπει να περιλαμβάνει τα ελάχιστα προβλεπόμενα στοιχεία προκειμένου να καθορίζονται επακριβώς οι υποχρεώσεις και οι ευθύνες εκάστου μέρους με απώτατο σκοπό την προστασία των δεδομένων των υποκειμένων.

Αδήριτη ανάγκη καθίσταται, και στο πλαίσιο του metaverse η διασφάλιση ότι μπορούν να ασκηθούν όλα τα σχετικά δικαιώματα που προβλέπει ο GDPR, στα άρθρα 12 επ., ήτοι δικαίωμα ενημέρωσης και διαφάνεια (άρθρα 12-14 GDPR), δικαίωμα πρόσβασης του υποκειμένου των δεδομένων (άρθρο 15 GDPR), δικαίωμα διόρθωσης (άρθρο 16 GDPR), δικαίωμα στη λήθη (άρθρο 17 GDPR), δικαίωμα περιορισμού της επεξεργασίας (άρθρο 18 GDPR), δικαίωμα στη φορητότητα των δεδομένων (άρθρο 18 GDPR), δικαίωμα εναντίωσης (άρθρο 21 GDPR) καθώς και δικαίωμα στη μη αυτοματοποιημένη ατομική λήψη αποφάσεων (άρθρο 22 GDPR).

Το ζήτημα ιδίως της αυτοματοποιημένης λήψης αποφάσεων αποκτά ιδιαίτερη σημασία εντός του metaverse καθώς προκειμένου οι πλατφόρμες να δρουν σύννομα θα πρέπει να ενημερώνουν τους χρήστες με σαφήνεια και διαφάνεια για την αυτοματοποιημένη λήψη αποφάσεων με βάση τα δεδομένα που έχουν στη διάθεσή τους. Ειδικότερα, όπως προαναφέρθηκε, η ανάλυση των κινήσεων των ματιών ενός χρήστη δεν συνδράμει μόνο στην ταυτοποίηση τούτου αλλά και στην εν συνεχεία εξαγωγή διαφόρων συμπερασμάτων π.χ. σχετικά με τις καταναλωτικές του συνήθειες ενώ έχει εν γένει αποδειχθεί ότι οι τεχνολογίες παρακολούθησης των ματιών έχουν τη δυνατότητα να προβούν σε πρόβλεψη των αποφάσεων των ατόμων μετά την πάροδο τριών δευτερολέπτων[158]. Ως εκ τούτου, κρίνεται αναγκαίο ο χρήστης να είναι ενήμερος για τέτοιου είδους καταστάσεις κατά τη χρήση του metaverse και να του έχει προηγουμένως

[158] Petrányi, D., Horváth, K. and Domokos, M. (2022) 'Part 3 - Data protection challenges, the importance of cybersecurity, advertising regulation in the metaverse'. Διαθέσιμο σε: https://cms.law/en/int/publication/legal-issues-in-the-metaverse/part-3-data-protection-challenges-the-importance-of-cybersecurity-advertising-regulation-in-the-metaverse (Τελευταία πρόσβαση: 14.06.2023)

επισημανθεί η δυνατότητα εναντίωσης στην εμπορική προώθηση βασιζόμενη στην κατάρτιση προφίλ καθώς και στην αυτοματοποιημένη ατομική λήψη αποφάσεων[159].

Ωστόσο, σε περιβάλλοντα, όπως το metaverse ενδέχεται να μην είναι σε όλες τις περιπτώσεις πάντοτε τόσο απλή η ικανοποίηση των ως άνω δικαιωμάτων π.χ. το δικαίωμα στη λήθη δεν μπορεί να ικανοποιηθεί στο πλαίσιο της τεχνολογίας blockchain, η οποία χρησιμοποιείται εντός του metaverse καθώς είναι μόνιμη η καταγραφή των συναλλαγών λόγω του αμετάβλητου χαρακτήρα του blockchain[160]. Ειδικότερα, λόγω της αμεταβλητότητας του χαρακτήρα της τεχνολογίας blockchain, σημαίνει ότι τούτη είναι αδύνατο να αλλοιωθεί, καταλήγοντας στην ύπαρξη ενός μόνιμου ιστορικού[161].

Πέραν της εξασφάλισης της άσκησης των δικαιωμάτων των υποκειμένων, οι εταιρείες θα πρέπει να διασφαλίζουν ότι τηρούνται όλες οι αρχές που προβλέπει ο GDPR, π.χ. ενδεικτικά η αρχή της ελαχιστοποίησης, η οποία προβλέπει ότι πρέπει να συλλέγονται όσο γίνεται λιγότερα προσωπικά δεδομένα, εφόσον αρκούν για την εκάστοτε πράξη επεξεργασίας και επομένως, σε περιπτώσεις που εντός του metaverse μπορεί να αποφευχθεί η αναγκαιότητα επεξεργασίας ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα, τότε πρέπει να αποφευχθεί η εν λόγω επεξεργασία. Με την τήρηση των εν λόγω αρχών προστατεύονται τόσο τα δικαιώματα των υποκειμένων των δεδομένων ενώ παράλληλα υπάρχει κανονιστική συμμόρφωση των εταιρειών καθώς και οικοδόμηση της εμπιστοσύνης έναντι των χρηστών[162].

Αξίζει να σημειωθεί ότι η λειτουργία του metaverse επιτάσσει την ανάγκη για ύπαρξη αυξημένων τεχνικών και οργανωτικών μέτρων εκ μέρους των υπεύθυνων επεξεργασίας, σύμφωνα με το άρθρο 24 του GDPR καθώς και την υιοθέτηση των αρχών της προστασίας

---

[159] Καρδαμάκη, Α. (2022), ό.π., σελ. 18

[160] Petrányi, D., Horváth, K. and Domokos, M. (2022) 'Part 3 - Data protection challenges, the importance of cybersecurity, advertising regulation in the metaverse', ό.π.

[161] Θεοδωράκης, Ν. και Καλογεράκης, Γ. (2019) 'Blockchain: εφαρμογές, προοπτικές και προκλήσεις για το ελληνικό νομικό σύστημα – Ιδίως οι εφαρμογές του στις έννομες σχέσεις ιδιωτικού δικαίου', *ΔΙΤΕ (π. ΔΙΜΕΕ)*, 16 (1). Διαθέσιμο σε: https://www.academia.edu/40377994/%CE%9A%CE%B1%CE%BB%CE%BF%CE%B3%CE%B5%CF%81%CE%AC%CE%BA%CE%B7%CF%82_%CE%98%CE%B5%CE%BF%CE%B4%CF%89%CF%81%CE%AC%CE%BA%CE%B7%CF%82_Blockchain_%CE%B5%CF%86%CE%B1%CF%81%CE%BC%CE%BF%CE%B3%CE%AD%CF%82_%CF%80%CF%81%CE%BF%CE%BF%CF%80%CF%84%CE%B9%CE%BA%CE%AD%CF%82_%CE%BA%CE%B1%CE%B9_%CF%80%CF%81%CE%BF%CE%BA%CE%BB%CE%AE%CF%83%CE%B5%CE%B9%CF%82_%CE%B3%CE%B9%CE%B1_%CF%84%CE%BF_%CE%B5%CE%BB%CE%BB%CE%B7%CE%BD%CE%B9%CE%BA%CF%8C_%CE%BD%CE%BF%CE%BC%CE%B9%CE%BA%CF%8C_%CF%83%CF%8D%CF%83%CF%84%CE%B7%CE%BC%CE%B1_%CE%94i%CE%9C%CE%95%CE%95_2019_%CF%83_5%CE%B5%CF%80 (Τελευταία πρόσβαση: 10.06.2023), σελ.21

[162] Cheong, B.C. (2022), ό.π., σελ. 491

από τον σχεδιασμό και εξ ορισμού[163]. Όπως έχει καταστεί σαφές, μέσω του metaverse δύνανται να συλλέγονται πολύ περισσότερα δεδομένα προσωπικού χαρακτήρα ειδικών κατηγοριών σε σύγκριση με τα σημερινά συστήματα και έτσι υπάρχει μεγαλύτερη ανάγκη για προστασία της ιδιωτικότητας των χρηστών. Επομένως, με σκοπό την προστασία των προσωπικών δεδομένων και δη τούτων που υπάγονται στις ειδικές κατηγορίες, θα πρέπει να λαμβάνονται μέτρα όπως ψευδωνυμοποίηση, κρυπτογράφηση, ελεγχόμενη πρόσβαση, έλεγχος ταυτότητας[164].

Περαιτέρω, αναγκαία στο πλαίσιο αυτό είναι και η λήψη μέτρων ελαχιστοποίησης της επεξεργασίας και μέτρων διαφάνειας της ενώ λόγω επεξεργασίας βιομετρικών δεδομένων ενώ θα πρέπει όλες οι επιχειρήσεις που δραστηριοποιούνται στον εν λόγω τομέα να διατηρούν αρχείο δραστηριοτήτων, σύμφωνα με το άρθρο 30 παρ. 5 του GDPR και να προβαίνουν σε διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία των δεδομένων (DPIA) καθώς μέσω του metaverse γίνεται χρήση νέων τεχνολογιών και αναμφίβολα υφίσταται υψηλός κίνδυνος για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων[165], στοιχεία τα οποία συνδράμουν δυναμικά στην κρίση του αν απαιτείται ή όχι DPIA.

Επισημαίνεται εκ νέου ότι η επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων, όπως είναι τα βιομετρικά δεδομένα που τυγχάνουν συλλογής εξ αφορμής του metaverse από τις συσκευές μπορούν να δημιουργήσουν πολλαπλούς κινδύνους για τις προσωπικές πτυχές του ψυχισμού των χρηστών. Στο πλαίσιο αυτό, οι συσκευές θα πρέπει να σχεδιάζονται με τρόπο που να τηρεί τις αρχές προστασίας των προσωπικών δεδομένων και την ιδιωτική ζωή των ατόμων χρηστών και να προβαίνει σε λεπτομερή έλεγχο των δεδομένων που έχουν συλλεχθεί, κάτι το οποίο θα μπορούσε να υλοποιηθεί μέσω τεχνολογιών ενίσχυσης της ιδιωτικότητας (PETs)[166], οι οποίες δύνανται να μειώσουν τους κινδύνους που σχετίζονται με την παραβίαση των προσωπικών δεδομένων.

Αναφορικά με το ζήτημα της επίτευξης διαλειτουργικότητας, της μεταφοράς και κοινής χρήσης των δεδομένων καθώς και των περιουσιακών στοιχείων, έχουν ήδη αναφερθεί ανωτέρω οι κίνδυνοι και οι ευπάθειες που μπορούν να ανακύψουν εξ αφορμής των εν λόγω πράξεων επεξεργασίας. Ως εκ τούτου, καθίσταται αναγκαία η ύπαρξη

[163] Καρδαμάκη, Α. (2022), ό.π., σελ. 18
[164] Dwivedi, K. Y. et al. (2022), ό.π., σελ. 8
[165] Καρδαμάκη, Α. (2022), ό.π., σελ. 19
[166] Fernandez, C.B and Hui, P. (2022), ό.π., σελ. 273

αναλυτικών συμφωνιών ανταλλαγής δεδομένων μεταξύ των πλατφορμών προκειμένου να καθορίζονται με ακρίβεια οι επιμέρους υποχρεώσεις αναφορικά με τη διασφάλιση της προστασίας των προσωπικών δεδομένων κατά τη μεταφορά από τη μία πλατφόρμα στην άλλη και με ενδεχόμενο καθορισμό των προτύπων ασφαλείας των δεδομένων ενώ αναγκαίος καθίσταται, και στο πλαίσιο των εν λόγω συμφωνιών, ο καθορισμός των ευθυνών μεταξύ των πλατφορμών ιδίως κατά την παραβίαση των δεδομένων προσωπικού χαρακτήρα[167]. Οι ως άνω συμφωνίες θα πρέπει, επίσης, να προβλέπουν μέτρα για την προστασία των δεδομένων καθώς και αναφορά για τα ζητήματα συγκατάθεσης των χρηστών και ενημέρωση τούτων σχετικά με τη μεταφορά των δεδομένων τους[168].

Προκειμένου να διασφαλιστεί η συμμόρφωση με την ισχύουσα νομοθεσία περί προστασίας των δεδομένων και να υπάρξει ασφάλεια δικαίου συνίσταται κατά μία άποψη «*η υιοθέτηση κωδίκων δεοντολογίας και μηχανισμών πιστοποίησης*» [169]. Περαιτέρω η ύπαρξη ενός αποκεντρωμένου μοντέλου metaverse που βασίζεται στην τεχνολογία blockchain και είναι διαλειτουργικό, θα μπορούσε καταρχήν να αντιμετωπίσει καλύτερα τα ζητήματα προστασίας των δεδομένων καθώς οι ίδιοι οι χρήστες θα μπορούσαν να διατηρούν τον έλεγχο των δεδομένων τους σε αντίθεση με πιο συγκεντρωτικά μοντέλα. Ωστόσο, εν προκειμένω τίθεται εκ νέου το ζήτημα της σύγκρουσης μεταξύ της τεχνολογίας blockchain και του GPDR[170] ιδίως αναφορικά με το δικαίωμα διαγραφής του υποκειμένου των δεδομένων.

Σε περίπτωση που όλα εκ των ως άνω μέτρων κρίνονται ανεπαρκή πάντοτε υφίσταται η δυνατότητα αναθεώρησης του υφιστάμενου πλαισίου περί προστασίας των προσωπικών δεδομένων. Ειδικότερα, το Ευρωπαϊκό Κοινοβούλιο επεσήμανε ότι το υφιστάμενο σχετικό νομικό καθεστώς εφαρμόζεται και στο metaverse και ζήτησε από την Επιτροπή να επιτύχει τη διασφάλιση της συμμόρφωσης των εμπλεκόμενων εντός του metaverse εταιρειών με το εν λόγω νομοθετικό καθεστώς. Ωστόσο, δεν πρέπει να αγνοηθεί το γεγονός ότι το metaverse παρουσιάζει μια σειρά προκλήσεων και ιδιαιτεροτήτων, οι οποίες δεν ήταν γνωστές κατά την υιοθέτηση του GDPR, ο οποίος δεν είχε σχεδιαστεί για να καλύπτει και τις εν λόγω πτυχές. Συνεπώς, πάντοτε υφίσταται ως λύση και η επικαιροποίηση και ο εκσυγχρονισμός του GDPR, για να καλύψει π.χ. περιπτώσεις όπως

[167] Gordon, M. (2022), ό.π., σελ.4
[168] Madiega, T., Car, P. et aI., (2022), ό.π., σελ. 5
[169] Madiega, T., Car, P. et aI., (2022), ό.π., σελ.6
[170] Madiega, T., Car, P. et aI., (2022), ό.π., σελ.6

ρύθμιση των συλλεχθέντων δεδομένων «*κατά τη διάρκεια ασυνείδητης συμπεριφοράς*»[171] ενώ καίριο είναι και το ζήτημα της χρήσης τεχνητής νοημοσύνης εντός του metaverse οπού αναδεικνύει την ανάγκη σύμπλευσης των νέων νομοθετημάτων, ήτοι της AI Act με τον GDPR.

[171] Madiega, T., Car, P. et aI., (2022), ό.π.

4. METAVERSE ΚΑΙ ΖΗΤΗΜΑΤΑ ΕΥΘΥΝΗΣ

Πέραν της ευθύνης, η οποία μπορεί να προκύψει στο πλαίσιο των προσωπικών δεδομένων, εις βάρος, είτε του υπευθύνου, είτε του εκτελούντος την επεξεργασία λόγω παραβίασης της συμμόρφωσής τους ως προς την προστασία των προσωπικών δεδομένων, ενδέχεται να ανακύψουν και άλλες περιπτώσεις ευθύνης στο metaverse ιδίως, είτε από τη μεριά των ίδιων των χρηστών – άβαταρ, είτε από τη μεριά των εταιρειών που διαχειρίζονται και στις οποίες ανήκουν οι εκάστοτε πλατφόρμες metaverse. Εν γένει, η κατανομή της ευθύνης μεταξύ των φορέων εκμετάλλευσης των πλατφορμών και των χρηστών είναι αρκετά δυσχερής ιδίως στο πλαίσιο των πλατφορμών κοινωνικής δικτύωσης και ηλεκτρονικού εμπορίου[172], πολλώ δε μάλλον στο metaverse.

4.1. Ευθύνη των χρηστών - άβαταρ

Με δεδομένο λοιπόν ότι οι χρήστες επί της ουσίας θα ζουν μια δεύτερη παράλληλη ζωή στο metaverse, εντός της οποίας, όπως σημειώθηκε ανωτέρω, θα προβαίνουν σε καθημερινές δραστηριότητες σαν εκείνες του πραγματικού κόσμου π.χ. αγοραπωλησία ακινήτων, ρούχων, έργων τέχνης[173], σύναψη συμβάσεων μέσω των άβαταρ τους, ενδέχεται να προκύψουν διάφορες διαμάχες, οι οποίες αν λάμβαναν χώρα στο φυσικό κόσμο θα ανέκυπτε νομοθετική παραβίαση. Οι ως άνω διαμάχες εκ μέρους ενός άβαταρ θα μπορούσαν να επηρεάσουν, είτε κάποιο άλλο άβαταρ, είτε μια εγκατάσταση του metaverse, είτε τον ίδιο το χρήστη, ήτοι το φυσικό πρόσωπο που υφίσταται πίσω από το άβαταρ καθώς και τρίτα πρόσωπα του πραγματικού κόσμου[174].

Θα μπορούσαν, συνεπώς, να προκύψουν περιστατικά που να θέτουν ζητήματα αστικής ευθύνης εντός του metaverse εστιάζοντας κυρίως στη διερεύνηση του μέρους που προέβη στη ζημιογόνο ενέργεια[175]. Σημειωτέον ότι οι γενικοί κανόνες περί αδικοπρακτικής ευθύνης καθώς και το δίκαιο των συμβάσεων θα μπορούσε να εφαρμοστεί κανονικά και στο metaverse, αν και τα δικαστήρια θα πρέπει να βρίσκονται σε ετοιμότητα να προσαρμόζουν τις υφιστάμενες ρυθμίσεις στις ιδιαιτερότητες της νέας αυτής τεχνολογίας[176] προκειμένου

---

[172] Dwivedi, K. Y. et al. (2022), ό.π., σελ. 11

[173] Sampaio, G. and Vaz M.C. (2022), 'Civil liability in the Metaverse'. Διαθέσιμο σε: https://www.bmalaw.com.br/en-US/pi/conteudo/contencioso-e-arbitragem/civil-liability-in-the-metaverse (Τελευταία πρόσβαση: 14.06.2023)

[174] Cheong, B.C. (2022), ό.π., σελ. 481

[175] Sampaio, G. and Vaz M.C. (2022), ό.π.

[176] Maciejewski, M. (2023), ό.π., σελ. 46

να εφαρμόζονται ορθά οι ως άνω κανόνες. Ωστόσο, πέραν από τα ζητήματα του αστικού δικαίου, ενδέχεται να ανακύψουν και περιστατικά που θα παραβίαζαν το ποινικό δίκαιο στον πραγματικό κόσμο[177]. Ειδικότερα, μπορεί να ανακύψουν παράνομες πράξεις όπως ανθρωποκτονία ή βιασμός εντός του metaverse[178]. Επομένως, με δεδομένο ότι τέτοιου είδους καταστάσεις θα ανέκυπταν και εντός του metaverse, είναι πολύ κρίσιμο να διαπιστωθεί αν μπορούν τα άβαταρ να έχουν δικαιώματα άξια προστασίας εντός του metaverse και αν καθίστανται τα ίδια τα άβαταρ υπεύθυνα για τις παράνομες ενέργειες τους στο metaverse καθώς και κατά πόσο είναι εύκολο να υλοποιηθεί η απόδοση ευθύνης στα άβαταρ με δεδομένο ότι αν τους αποδοθεί ευθύνη θα είναι σαν να διαθέτουν δικαιώματα και υποχρεώσεις, και άρα σαν να διαθέτουν νομική προσωπικότητα[179].

Το πιο μεγάλο ζήτημα, εν προκειμένω, είναι το πώς θα επιμεριστούν οι ευθύνες ιδίως κάνοντας χρήση των υφιστάμενων νομικών εννοιών και με την ταυτόχρονη ανάγκη προστασίας των δικαιωμάτων των χρηστών[180]. Για παράδειγμα σε ζητήματα ευθύνης των άβαταρ εντός του metaverse θα μπορούσαν αναλόγως της εκάστοτε περίπτωσης να εφαρμοστούν διατάξεις που προέρχονται επί παραδείγματι από το εταιρικό δίκαιο, περίπτωση, η οποία θα αναλυθεί κατωτέρω.

Τρεις είναι οι βασικοί τρόποι απόδοσης ευθύνης σε τέτοιου είδους περιπτώσεις, ήτοι στην περίπτωση, επομένως που προκύψει ζημιογόνο γεγονός εντός του metaverse, το οποίο ενδέχεται να επεκταθεί και στο φυσικό κόσμο, τότε η ευθύνη θα μπορούσε να επιβληθεί είτε στο ίδιο το άβαταρ, κάτι το οποίο όπως αναφέρθηκε, θα σήμαινε ότι το άβαταρ θα διέθετε νομική προσωπικότητα, είτε στους εφευρέτες και προγραμματιστές του metaverse, είτε τρίτον στο φυσικό πρόσωπο που υφίσταται πίσω από το άβαταρ[181].

Καταρχάς για να προσδιοριστεί αν μπορεί το άβαταρ να διαθέτει αντίστοιχα δικαιώματα με αυτά ενός φυσικού προσώπου, υφίσταται η άποψη ότι θα πρέπει καταρχήν να διαθέτει συνείδηση, κάτι το οποίο επί του παρόντος δεν συμβαίνει καθώς δεν διαθέτουν τα άβαταρ δική τους συνείδηση. Άλλο ένα κριτήριο, το οποίο συμβάλλει στο αν πρέπει να αποκτήσει το άβαταρ ξεχωριστή νομική προσωπικότητα είναι να συμφωνεί ο χρήστης -

---

[177] Cheong, B.C. (2022), ό.π., σελ. 472

[178] Τα εν λόγω ζητήματα αναλύονται διεξοδικά στο έκτο κεφάλαιο της παρούσας.

[179] Χιόνη, Γ. (2022) 'Δίκαιο και Μετασύμπαν (II): Το δίκαιο των avatar'. Διαθέσιμο σε: https://www.lawspot.gr/nomika-blogs/georgia_hioni/dikaio-kai-metasympan-ii-dikaio-ton-avatar (Τελευταία πρόσβαση: 11.06.2023)

[180] Cheong, B.C. (2022), ό.π., σελ. 471

[181] Cheong, B.C. (2022), ό.π., σελ. 481

δημιουργός του στην απόκτηση νομικής προσωπικότητας του άβαταρ που θα υπόκειται στους ξεχωριστούς νόμους του metaverse. Ίσως τα άβαταρ του μέλλοντος αποκτήσουν ξεχωριστή νομική προσωπικότητα, εφόσον δύνανται να εκτελούν διάφορες ενέργειες αυτοβούλως, κάνοντας χρήση τεχνολογιών τεχνητής νοημοσύνης. Στην περίπτωση αυτή θα είναι αναγκαία η ύπαρξη μιας νομοθεσίας που να επιλύει μια σειρά ζητημάτων, όπως τα πνευματικά δικαιώματα των άβαταρ[182].

Το πιο σημαντικό ζήτημα σε αυτή την περίπτωση, το οποίο έχει απασχολήσει εν γένει την ερευνητική κοινότητα είναι κατά πόσον τα συστήματα τεχνητής νοημοσύνης θα πρέπει να αποκτήσουν ξεχωριστή νομική προσωπικότητα. Εν προκειμένω, αν τα άβαταρ στο metaverse έχουν τη δυνατότητα να μπορούν να εκτελούν καθημερινές δραστηριότητες χωρίς ανθρώπινη παρέμβαση, άρα είναι εν τέλει ικανά για μηχανική μάθηση, τότε υπάρχει σκοπιμότητα να δοθούν στο άβαταρ δικαιώματα και υποχρεώσεις, σαν εκείνες που μπορεί να έχει ένα ανθρώπινο ον. Παρόλα αυτά, αν πίσω από το άβαταρ υπάρχει σύστημα τεχνητής νοημοσύνης του πραγματικού κόσμου ως χειριστής του άβαταρ αντί για ένα ανθρώπινο ον, το ζήτημα γίνεται ακόμα πιο περίπλοκο[183]. Και τούτο διότι, ήδη υφίστανται πολλοί προβληματισμοί στην ευθύνη των συστημάτων τεχνητής νοημοσύνης.

Γενικότερα, στο πλαίσιο αυτό, αξίζει να σημειωθεί ότι σε περιπτώσεις όπου εμπλέκονται συστήματα τεχνητής νοημοσύνης και προκαλούνται ζημίες, θα μπορούσε να εφαρμοστεί η AI Liability Directive[184] στις περιπτώσεις δηλαδή εκείνες κατά τις οποίες τίθενται ζητήματα ζημίας και συνεπώς ευθύνης από υπηρεσίες ή προϊόντα που βασίζονται στην τεχνητή νοημοσύνη προκειμένου να διευκολυνθεί το θύμα σε επίπεδο απόδειξης (βάρος απόδειξης και αποκάλυψη αποδεικτικών στοιχείων). Ειδικότερα, η εν λόγω Οδηγία προτάθηκε λόγω της μη επαρκούς κάλυψης εκ μέρους των υπαρχόντων κανόνων περί ευθύνης, οι οποίοι δημιουργούν δυσχερή ζητήματα λόγω της ανάγκης απόδειξης της υπαιτιότητας, την οποία πρέπει να αποδείξει ο ζημιωθείς σε περιπτώσεις που αιτείται αποζημίωση για τη ζημία που υπέστη, κάτι το οποίο φαίνεται δύσκολο όταν πρέπει να αποδειχθεί ζημία στην περίπτωση που παρεμβάλλεται σύστημα τεχνητής νοημοσύνης λόγω της ενδεχόμενης αδιαφάνειας των εν λόγω συστημάτων.

---

[182] Cheong, B.C. (2022), ό.π., σελ. 477

[183] Cheong, B.C. (2022), ό.π., σελ. 477

[184] Η AI Liability Directive λόγω του ότι συνιστά Οδηγία αφήνει περιθώρια επιμέρους ειδικότερων ρυθμίσεων εκ μέρους των κρατών μελών και ακολουθεί μια προσέγγιση ελάχιστης εναρμόνισης, σύμφωνα με την αιτιολογική σκέψη 14.

Επιπρόσθετα, υφίσταται η δυνατότητα δανεισμού εννοιών από το εταιρικό δίκαιο, οι οποίες θα μπορούσαν να δημιουργήσουν κάποιες λύσεις στο ζήτημα της ευθύνης του άβαταρ. Ειδικότερα, θα μπορούσαν να χορηγηθούν δικαιώματα στα άβαταρ, αντίστοιχα με τα δικαιώματα των εταιρειών[185]. Η εν λόγω νομική προσωπικότητα θα μπορούσε να δοθεί στο άβαταρ μέσω μιας διαδικασίας καταχώρισης, αντίστοιχης με αυτής, στην οποία προβαίνουν οι εταιρείες κατά την ίδρυσή τους στο πλαίσιο του εταιρικού δικαίου, λαμβάνοντας αριθμό μητρώου εντός του metaverse. Στην εν λόγω περίπτωση, το κάθε φυσικό πρόσωπο θα μπορούσε να δημιουργεί και να εγγράφει μόνο ένα άβαταρ στο αποκεντρωμένο metaverse[186]. Επιπλέον, στο πλαίσιο της καταχώρισης του άβαταρ με τη μορφή της εταιρείας θα μπορούσε να προβλέπεται και ελάχιστο κεφάλαιο σύστασης[187], αναλόγως και του είδους της εταιρείας και με σκοπό να καλύπτονται τυχόν αξιώσεις ευθύνης στο metaverse.

Επομένως, δύνανται να χρησιμοποιηθεί το μοντέλο των εταιρειών προκειμένου να παρασχεθούν δικαιώματα στα άβαταρ σε ένα metaverse καθώς μεταξύ εταιρειών και άβαταρ υφίστανται μια σειρά από ομοιότητες π.χ. και οι δύο έννοιες αφορούν σε μη ανθρώπινες οντότητες, δύνανται να αυξάνουν τις οικονομικές επενδύσεις[188] και ενώ και οι δύο ενεργούν μέσω άλλων προσώπων. Επίσης, καμία από τις δύο ως άνω οντότητες δεν διατρέχει κίνδυνο θανάτου ή σωματικής βλάβης[189].

Στο σημείο αυτό αξίζει να σημειωθεί ότι, όπως μπορεί να υπάρξει άρση της νομικής προσωπικότητας ενός νομικού προσώπου, έτσι μπορεί να συμβεί και με το άβαταρ, ιδίως σε περιπτώσεις σημαντικής ζημίας, όπου τούτη επεκτείνεται και στον πραγματικό κόσμο και τούτο διότι πρέπει να υπάρξει ένα πρόσωπο, στο οποίο θα επιβληθεί ευθύνη και το οποίο θα αποκαταστήσει τη ζημία. Άρα καταλήγουμε με αυτόν τον τρόπο, ότι την ευθύνη θα την αναλάβει το πρόσωπο που υφίσταται πίσω από το άβαταρ και άρα κατόπιν άρσης της τεχνικής προσωπικότητας που έχει δοθεί στο άβαταρ με αρχικό σκοπό τούτα να αποκτήσουν δικαιώματα και υποχρεώσεις. Με δεδομένο ότι ο βασικός ανησυχητικός λόγος είναι ότι οι χρήστες πίσω από τα άβαταρ θα δρουν ασυνείδητα και καταχρηστικά, έχοντας ως πέπλο τη ξεχωριστή νομική προσωπικότητα των άβαταρ, θα πρέπει να υπάρξει δυνατότητα άρσης της

[185] Cheong, B.C. (2022), ό.π., σελ. 471
[186] Cheong, B.C. (2022), ό.π., σελ. 478
[187] Cheong, B.C. (2022), ό.π., σελ. 476
[188] Cheong, B.C. (2022), ό.π., σελ. 478
[189] Cheong, B.C. (2022), ό.π., σελ. 482

εν λόγω τεχνητής νομικής προσωπικότητας, προκειμένου να μη δρουν οι χρήστες αυθαίρετα[190] και με σκοπό την επιβολή των αναγκαίων και απαραίτητων ευθυνών.

Περαιτέρω αναφορικά με την ευθύνη των ίδιων των χρηστών θα μπορούσε καταρχήν να αναγνωριστεί ένα «πέπλο ανωνυμίας»[191] στο πρόσωπο που υφίσταται πίσω από άβαταρ καθώς τα άβαταρ δεν αντιπροσωπεύουν αδιαμφισβήτητα τη συμπεριφορά του χρήστη στο φυσικό κόσμο υπό την έννοια ότι οι χρήστες δύνανται να συμπεριφέρονται με διαφορετικό τρόπο, ο οποίος να έρχεται εν τοις πράγμασι σε αντίθεση με τις συνήθειες τους αναφορικά με τις κοινωνικές τους αλληλεπιδράσεις στον πραγματικό κόσμο[192] χωρίς φυσικά να δρουν αυθαίρετα και καταχρηστικά προκαλώντας σημαντικές νομοθετικές παραβιάσεις. Στο πλαίσιο αυτό, το φυσικό πρόσωπο θα μπορούσε να υποστηρίξει ότι δεν μπορεί να είναι το ίδιο υπεύθυνο για πράξεις ή/και παραλείψεις του άβαταρ στο metaverse καθώς πρόκειται για ένα μη πραγματικό κόσμο. Ένα βασικό επιχείρημα, εν προκειμένω θα ήταν ότι ως πραγματικά εγκλήματα θεωρούνται αποκλειστικά εκείνα που λαμβάνουν χώρα στο φυσικό κόσμο[193]. Ωστόσο, επειδή «το πέπλο ανωνυμίας» δεν θα εφαρμόζεται από όλους τους χρήστες με ορθό τρόπο, αλλά τουναντίον μπορεί να υφίσταται μια σειρά δυσμενών και αυθαίρετων ενεργειών εκ μέρους του χρήστη που κρύβεται πίσω από το άβαταρ, οι οποίες δύνανται να προκαλέσουν άσκηση αυθαίρετης εξουσίας με σκοπό την επίτευξη προσωπικών ατομικών συμφερόντων εις βάρος των λοιπών χρηστών του metaverse[194], τότε είναι αμφίβολο κατά πόσο το εν λόγω πέπλο μπορεί και πρέπει πράγματι να προστατεύσει τον «κρυμμένο» πίσω από το άβαταρ χρήστη. Αντιστοίχως, σε περιπτώσεις που πίσω από ένα άβαταρ βρίσκεται μια εταιρεία του πραγματικού κόσμου που επιθυμεί να αυξήσει τις πωλήσεις της, τότε δεν θα μπορεί να καλύπτεται από τη δυνατότητα ανωνυμίας[195].

Υποστηρίζεται, λοιπόν, η άποψη ότι θα πρέπει να υφίστανται κάποιες διαφοροποιήσεις στο ζήτημα του κατά πόσον πρέπει να αποκαλύπτεται αυτοδικαίως η αληθινή ταυτότητα του άβαταρ, δηλαδή εφόσον δεν υφίσταται σαφής πρόθεση του χρήστη πίσω από το άβαταρ να συνδέσει την ταυτότητα του άβαταρ με την πραγματική του ταυτότητα, τότε θα μπορούσε να προστατευτεί από το πέπλο ανωνυμίας εκτός εάν προβαίνει σε πράξεις που αποσκοπούν σε παραβίαση του νόμου και πρόκληση

[190] Cheong, B.C. (2022), ό.π., σελ. 493-494
[191] Cheong, B.C. (2022), ό.π., σελ. 480
[192] Dwivedi, K. Y. et al. (2022), ό.π., σελ. 11
[193] Cheong, B.C. (2022), ό.π., σελ. 482
[194] Cheong, B.C. (2022), ό.π., σελ. 472
[195] Cheong, B.C. (2022), ό.π., σελ. 480

αδικοπραξίας που δημιουργεί έννομες συνέπειες και στο φυσικό κόσμο λόγω της παράνομης συμπεριφοράς του άβαταρ εντός του metaverse, τότε ο χρήστης πίσω από το άβαταρ με μεγάλη βεβαιότητα θα πρέπει να θεωρηθεί ως υπεύθυνος για την αδικοπρακτική ζημία που προκάλεσε το άβαταρ του εις βάρος άλλων χρηστών – άβαταρ στο metaverse[196].

Στο πλαίσιο αυτό, παρατηρείται ότι οι κακόβουλοι χρήστες προστατευόμενοι από την ανωνυμία μέσω του άβαταρ τους θα προκαλούσαν ταυτόχρονα το μεγάλο ζήτημα του πώς θα αποκατασταθεί η εν λόγω ζημία, η οποία με δύσκολο τρόπο θα μπορούσε να αποκατασταθεί με δεδομένη την ύπαρξη δυσκολίας περί της άμεσης διαπίστωσης αναφορικά με το ποιος κρύβεται πίσω από τη ζημιογόνο ενέργεια. Η εν λόγω κατάσταση μπορεί να επιδεινωθεί, εφόσον ένας χρήστης κατορθώσει να δημιουργήσει περισσότερα του ενός άβαταρ προκειμένου να προβαίνει σε παράνομες συμπεριφορές. Κρίσιμος θα είναι και ο καθορισμός του πταίσματος (ύπαρξη δόλου ή αμέλειας) καθώς και ο προσδιορισμός περί της αποκατάστασης της προκληθείσας ζημίας, η οποία αμφιταλαντεύεται μεταξύ του εικονικού και του φυσικού κόσμου, κάτι το οποίο θέτει εκ νέου το ζήτημα του εφαρμοστέου δικαίου στο πλαίσιο της αστικής ευθύνης εντός του metaverse, ιδίως π.χ. όταν υφίστανται και περιπτώσεις ηθικής βλάβης[197]. Θα μπορούσε, άλλωστε, η ευθύνη του φυσικού προσώπου να καθορίζεται κλιμακωτά αναλόγως της ζημίας που προκλήθηκε τόσο στο metaverse αλλά και με βάση τις επιπτώσεις αυτής στον πραγματικό κόσμο[198].

Αξίζει να σημειωθεί ότι αναφορικά με την ευθύνη των προγραμματιστών, τούτοι θα μπορούσαν να απαλλαγούν από την απεριόριστη ευθύνη τους ιδίως με σκοπό τη διατήρηση του κινήτρου τους για συνεχή καινοτομία εντός του περιβάλλοντος του metaverse[199]. Άλλωστε, υπάρχει έντονα η άποψη ότι οι προγραμματιστές και οι εφευρέτες δεν πρέπει να θεωρούνται υπεύθυνοι για τις πράξεις των άβαταρ καθώς αυτά δεν ελέγχονται άμεσα από τους ίδιους αλλά από τους χρήστες[200]. Περαιτέρω, αν και σε περιπτώσεις π.χ. ψυχικής ζημίας προκληθείσας από ένα παιχνίδι, έχει παρατηρηθεί ότι ευθύνεται, είτε ο κατασκευαστής, είτε ο διανομέας του παιχνιδιού, σε αποκεντρωμένα συστήματα, όπως το metaverse θα ήταν εξαιρετικά δύσκολο να εντοπιστεί ο κατασκευαστής προκειμένου να του αποδοθεί ευθύνη[201].

[196] Cheong, B.C. (2022), ό.π.
[197] Sampaio, G. and Vaz M.C. (2022), ό.π.
[198] Cheong, B.C. (2022), ό.π., σελ. 475
[199] Cheong, B.C. (2022), ό.π., σελ. 480
[200] Cheong, B.C. (2022), ό.π., σελ. 477
[201]Cheong, B.C. (2022), ό.π., σελ. 476

4.2. Ευθύνη των παρόχων - εταιρειών

Πέραν της ευθύνης των χρηστών για πράξεις και αδικήματα τους εντός του metaverse, δεν μπορεί να αποκλειστεί και ευθύνη των εταιρειών παρόχων της ίδιας της πλατφόρμας του metaverse, ιδίως αναφορικά με το παράνομο περιεχόμενο εντός του metaverse. Στο πλαίσιο αυτό, τυχόν ζητήματα ευθύνης των παρόχων της πλατφόρμας του metaverse θα μπορούσαν να ρυθμιστούν μέσω της DSA, η οποία δύναται να εφαρμοστεί και στο metaverse και καθώς πρόκειται για Κανονισμό, έχει άμεση και ευθεία εφαρμογή με σκοπό την εναρμόνιση των εθνικών αγορών. Η DSA έχει ως βασική αρχή ότι «*ό,τι είναι παράνομο εκτός διαδικτύου, θα πρέπει να είναι παράνομο και στο διαδίκτυο*»[202] ενώ μέσω αυτής επιδιώκεται η εξισορρόπηση της ευθύνης τόσο των χρηστών, όσο και των πλατφορμών καθώς και των δημοσίων αρχών με βασικότερο στόχο την προστασία των καταναλωτών[203]. Αποτελεί την εξέλιξη της Οδηγίας για το ηλεκτρονικό εμπόριο[204]. Ειδικότερα, η DSA, αποσκοπεί, μεταξύ άλλων, στην καθιέρωση μιας σειράς ευθυνών και ενός ξεκάθαρου και αυστηρότερου πλαισίου λογοδοσίας καθώς και διαφάνειας για τους παρόχους υπηρεσιών διαμεσολάβησης[205]. Εστιάζει δε στη θέσπιση νέων προβλέψεων προς αντιμετώπιση του παράνομου διαδικτυακού περιεχομένου και ταυτόχρονα στον καθορισμό των υποχρεώσεων των πλατφορμών, όπως τούτες περιγράφονται ενδεικτικά κατωτέρω[206].

Στο πλαίσιο αυτό, ενδυναμώνονται δε και καθίστανται πιο σαφείς οι προϋποθέσεις περί απαλλαγής από την ευθύνη των πλατφορμών και άλλων ενδιάμεσων φορέων, οι οποίοι καταρχήν δεν θα θεωρούνται υπεύθυνοι για παράνομη συμπεριφορά των χρηστών, εκτός

---

[202] Συμβούλιο της ΕΕ (2021), *Ό,τι είναι παράνομο εκτός διαδικτύου θα πρέπει να είναι παράνομο και στο διαδίκτυο: Καθορισμός της θέσης του Συμβουλίου σχετικά με την πράξη για τις ψηφιακές υπηρεσίες.* Διαθέσιμο σε: https://www.consilium.europa.eu/el/press/press-releases/2021/11/25/what-is-illegal-offline-should-be-illegal-online-council-agrees-on-position-on-the-digital-services-act/ (Τελευταία πρόσβαση: 16.06.2023)

[203] Ευρωπαϊκή Επιτροπή (2023), *Πράξη για τις ψηφιακές υπηρεσίες: διασφάλιση ενός ασφαλούς και υπεύθυνου διαδικτυακού περιβάλλοντος.* Διαθέσιμο σε: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_el (Τελευταία πρόσβαση: 16.06.2023)

[204] *Οδηγία 2000/31/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 8ης Ιουνίου 2000 για ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά («οδηγία για το ηλεκτρονικό εμπόριο»).* Διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=celex:32000L0031 (Τελευταία πρόσβαση: 16.06.2023)

[205] Angeles, J. (2022). 'The EU legal obligations of very large platforms providing digital services in the age of the metaverse'. *Cuadernos de Derecho Transnacional*, 14(2), 294-318. Διαθέσιμο σε: CUADERNOS DE DERECHO TRANSNACIONAL (uc3m.es) (Τελευταία πρόσβαση: 16.06.2023), σελ.294

[206] Angeles, J. (2022), ό.π., σελ. 298

εάν οι ως άνω φορείς έχουν λάβει γνώση της εν λόγω παρανομίας και δεν προέβησαν σε εξάλειψη αυτής[207], επομένως κρίσιμα είναι τα στοιχεία του ενεργού ρόλου και της γνώσης. Αντίστοιχα με τις προβλέψεις της Οδηγίας περί του ηλεκτρονικού εμπορίου, η DSA προβλέπει τις εξαιρέσεις από την ευθύνη των ενδιάμεσων φορέων, οι οποίοι είτε προβαίνουν σε απλή μετάδοση (άρθρο 4 DSA), είτε σε προσωρινή αποθήκευση (άρθρο 5 DSA), είτε σε παροχή φιλοξενίας για την ύπαρξη παράνομου περιεχομένου (άρθρο 6 DSA).

Επομένως, αναλόγως των ενεργειών του εκάστοτε παρόχου ενδιάμεσων υπηρεσιών π.χ. απλή μετάδοση, υφίστανται ειδικότερες προβλέψεις εντός της DSA. Καταρχήν γίνεται σαφές ότι ένας πάροχος ενδιάμεσων υπηρεσιών δύναται να απαλλαγεί της ευθύνης του, εφόσον, στην περίπτωση της απλής μετάδοσης και προσωρινής αποθήκευσης, δεν επεμβαίνει με οιονδήποτε τρόπο στις μεταδιδόμενες ή προσβάσιμες πληροφορίες[208]. Στον αντίποδα, όταν υφίσταται σκόπιμη συνεργασία του παρόχου ενδιάμεσων υπηρεσιών με τον αποδέκτη των υπηρεσιών προκειμένου να διενεργηθούν παράνομες δραστηριότητες, τότε ουδεμία απαλλαγή από την ευθύνη του παρόχου επέρχεται[209]. Σύμφωνα με την αιτιολογική σκέψη 22 της DSA, στην περίπτωση του παρόχου υπηρεσιών φιλοξενίας, όταν τούτος αποκτήσει πραγματική γνώση ή καταλάβει ότι προβαίνει σε επεξεργασία ή αποθήκευση παράνομων πληροφοριών οφείλει να δράσει άμεσα κατόπιν λήψης κατάλληλων μέτρων προκειμένου να αφαιρείται το περιεχόμενο ή να μη δύναται κάποιος να έχει πρόσβαση σε τούτο τηρουμένης μιας σειράς ουσιωδών αρχών των αποδεκτών της υπηρεσίας, όπως π.χ. αρχή ελευθερίας και έκφρασης. Σημειωτέον ότι το γεγονός ότι γενικά υφίσταται γνώση του παρόχου περί του ότι η υπηρεσία του τυγχάνει χρήσης, μεταξύ άλλων, και με σκοπό την αποθήκευση παράνομου περιεχομένου δεν πληροί άνευ ετέρου την απόκτηση της πραγματικής γνώσης ή επίγνωσης του παρόχου με την παραπάνω έννοια[210].

Περαιτέρω, οι ως άνω περιπτώσεις απαλλαγής από την ευθύνη δεν αποκλείουν άνευ ετέρου τη δυνατότητα των κρατών μελών να επιβάλλουν προσωρινά μέτρα στους παρόχους υπηρεσιών διαμεσολάβησης εντός του metaverse π.χ. απαίτηση των εκάστοτε εθνικών δικαστηρίων ή/και αρμοδίων διοικητικών αρχήν περί της αφαίρεσης περιεχομένου ή της

---

[207] Ευρωπαϊκή Επιτροπή, *Μια Ευρώπη έτοιμη για την ψηφιακή εποχή: νέοι κανόνες για τις διαδικτυακές πλατφόρμες.* Διαθέσιμο σε: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment/europe-fit-digital-age-new-online-rules-platforms_el (Τελευταία πρόσβαση: 16.06.2023)

[208] Αιτιολογική Σκέψη 21 DSA

[209] Αιτιολογική Σκέψη 20 DSA.

[210] Αιτιολογική Σκέψη 22 DSA

άρνησης πρόσβασης σε τούτο δίχως να υφίσταται αντίθεση με το δίκαιο της Ένωσης[211]. Ωστόσο, το πρόβλημα των παράνομων δραστηριοτήτων και του παράνομου περιεχομένου, ακόμα και εντός του metaverse δεν μπορεί να επιλυθεί επικεντρωμένοι αποκλειστικά και μόνο στην ευθύνη των παρόχων ενδιάμεσων υπηρεσιών και επομένως τρίτα θιγόμενα από παράνομο περιεχόμενο μέρη οφείλουν να διερευνούν τη δυνατότητα επίλυσης χωρίς τη συμμετοχή των εν λόγω παρόχων ενώ δεν αποκλείεται και η ευθύνη των αποδεκτών της υπηρεσίας[212].

Επομένως, συνάγεται ότι δεν είναι ορθό εξ αρχής ο ενδιάμεσος πάροχος να θεωρείται υπεύθυνος για το παράνομο περιεχόμενο που προέρχεται από τους αποδέκτες της υπηρεσίας καθώς σε διαφορετική περίπτωση, οι εταιρείες τεχνολογίας διαχειρίστριες των εκάστοτε πλατφορμών που συναποτελούν το metaverse θα επηρεάζονταν σε δυσανάλογο βαθμό[213]. Σε κάθε περίπτωση, όπως προαναφέρθηκε, και σύμφωνα με την αιτιολογική σκέψη 18 DSA, «*οι απαλλαγές από την ευθύνη ….. δεν θα πρέπει να εφαρμόζονται όταν ο πάροχος ενδιάμεσων υπηρεσιών, αντί να περιορίζεται στην παροχή των υπηρεσιών με ουδέτερο τρόπο με απλώς τεχνική και αυτόματη επεξεργασία των πληροφοριών που παρέχονται από τον αποδέκτη της υπηρεσίας, διαδραματίζει ενεργό ρόλο ο οποίος είναι τέτοιας φύσεως ώστε να του παρέχει γνώση ή έλεγχο των εν λόγω πληροφοριών*». Συνεπώς, εφόσον ο πάροχος της πλατφόρμας metaverse παρέχει τις υπηρεσίες με ουδέτερο τρόπο και δεν είχε ενεργό ρόλο επί του παράνομου περιεχομένου, δύναται να απαλλαγεί από τη σχετική ευθύνη του.

Αξίζει να σημειωθεί ότι η DSA προκειμένου να ενισχύσει την προστασία των χρηστών στο διαδίκτυο και να επιμερίσει την ευθύνη μεταξύ των μερών επιβάλλει μια σειρά υποχρεώσεων δέουσας επιμέλειας στους παρόχους αναλόγως τις κατηγορίας στην οποία υπάγονται (Κεφάλαιο ΙΙΙ DSA)[214]. Στο πεδίο του metaverse, ως δέουσα επιμέλεια, θα μπορούσαν εν γένει να θεωρηθούν κάποια απαραίτητα και αποτελεσματικά μέτρα, τα οποία καλούνται να λάβουν οι τεχνολογικές εταιρείες διαχειρίστριες του metaverse, μέτρα τα οποία θα σκοπούν, ενδεικτικά, στην πρόληψη, μετριασμό ή περιορισμό του παράνομου περιεχομένου καθώς και μέτρα για την αντιμετώπιση τυχόν αρνητικών επιπτώσεων στο

[211] Angeles, J. (2022), ό.π., σελ. 303
[212] Αιτιολογική Σκέψη 27 DSA
[213] Angeles, J. (2022), ό.π., σελ. 301-302
[214] Ενδεικτικά αναφέρονται μερικές εκ των υποπεριπτώσεων στο πλαίσιο των υποχρεώσεων.

πλαίσιο των δραστηριοτήτων τους[215]. Ειδικότερα, η DSA περιλαμβάνει ένα κατάλογο υποχρεώσεων που επιβάλλονται σε όλους του παρόχους ενδιάμεσων υπηρεσιών με σκοπό τη διασφάλιση «*ενός ελάχιστου βαθμού ασφάλειας δικαίου*»[216] π.χ. διορισμός ενιαίου σημείου επαφής. Περαιτέρω, υφίστανται ειδικότερες υποχρεώσεις π.χ. για τους παρόχους υπηρεσιών φιλοξενίας, όπως εφαρμογή μηχανισμών ειδοποίησης και δράσης, καθώς ο ρόλος των εν λόγω παρόχων είναι ιδιαίτερα σημαντικός στην καταπολέμηση του παράνομου περιεχομένου εντός του διαδικτύου λόγω των ενεργειών τους π.χ. παροχή πρόσβασης σε πληροφορίες άλλων αποδεκτών σε μεγάλη κλίμακα[217].

Επίσης, αξίζει να αναφερθεί και η περίπτωση της επιβολής επιπρόσθετων υποχρεώσεων στις λεγόμενες μεγάλες επιγραμμικές πλατφόρμες αυξάνοντας με αυτόν τον τρόπο τις ευθύνες τους[218] καθώς οι εν λόγω μεγάλες πλατφόρμες έχουν μεγάλη επιρροή τόσο έναντι των χρηστών όσο και εν γένει της αγοράς και ως εκ τούτου υπόκεινται σε υψηλές υποχρεώσεις διαφάνειας και λογοδοσίας, δίχως ωστόσο να προσδιορίζεται εντός του ίδιου του Κανονισμού το τι συνιστά παράνομο περιεχόμενο[219]. Η DSA επιβάλλοντας τις ως άνω υποχρεώσεις προσπαθεί να περιορίσει τις πολύ μεγάλες επιγραμμικές πλατφόρμες, ήτοι, μεταξύ άλλων, τους Big Tech και στο πλαίσιο αυτό η Επιτροπή έχει ήδη προσφάτως δημοσιεύσει τον κατάλογο με τις οντότητες που περιλαμβάνονται στην έννοια των πολύ μεγάλων επιγραμμικών πλατφορμών[220].

Σημαντική είναι η πρόβλεψη της DSA στο πεδίο της ευθύνης αναφορικά με τις εθελοντικές ενέργειες των παρόχων με σκοπό τη, μεταξύ άλλων, ανίχνευση παράνομου περιεχομένου (άρθρο 7 της DSA), οι οποίες καταρχήν «*δεν θα πρέπει να χρησιμοποιούνται για την παράκαμψη των υποχρεώσεων των παρόχων ενδιάμεσων υπηρεσιών*»[221] που προβλέπονται στη DSA αλλά ταυτόχρονα τέτοιου είδους δράσεις δεν συνεπάγονται αύξηση της ευθύνης τους. Εξίσου σημαντική είναι και η πρόβλεψη περί της μη επιβολής γενικής υποχρέωσης παρακολούθησης του περιεχομένου στους εν λόγω παρόχους και περί μη

---

[215] Angeles, J. (2022), ό.π., σελ. 303
[216] Angeles, J. (2022), ό.π.
[217] Αιτιολογική Σκέψη 50 DSA
[218] Ευρωπαϊκή Επιτροπή (2023), *Ερωτήσεις και απαντήσεις: πράξη για τις ψηφιακές υπηρεσίες.* Διαθέσιμο σε: https://ec.europa.eu/commission/presscorner/detail/el/QANDA_20_2348 (Τελευταία πρόσβαση: 16.06.2023)
[219] Angeles, J. (2022), ό.π., σελ. 300
[220] Ευρωπαϊκή Επιτροπή (2023), *Πράξη για τις ψηφιακές υπηρεσίες: η Επιτροπή ορίζει τις πρώτες πολύ μεγάλες επιγραμμικές πλατφόρμες και μηχανές αναζήτησης.* Διαθέσιμο σε: https://ec.europa.eu/commission/presscorner/detail/el/IP_23_2413 (Τελευταία πρόσβαση: 16.06.2023)
[221] Αιτιολογική Σκέψη 26 DSA

υποχρέωσης να αναζητούν με ενεργητικό τρόπο γεγονότα που συνιστούν παράνομη ενέργεια(άρθρο 8 της DSA), δηλαδή η DSA δεν προσπαθεί να επιβάλλει στους εν λόγω παρόχους την υποχρέωση να έχουν γενικότερη και διαρκή εποπτεία επί του περιεχομένου.

Αξίζει να σημειωθεί ότι, οι υπάρχουσες πλατφόρμες στο metaverse π.χ. Sandbox, Roblox, Decentraland προκειμένου να περιορίσουν τη δική τους ευθύνη έχουν εισάγει στους όρους χρήσης τους προβλέψεις περί αποποίησης της ευθύνης τους και επί της ουσίας προσπαθούν να εναποθέσουν με αυτό τον τρόπο την ευθύνη του περιεχομένου και της χρήσης της εκάστοτε πλατφόρμας metaverse στο χρήστη - καταναλωτή[222].

Επομένως, εντός του metaverse τίθενται αρκετά ζητήματα περί του βαθμού της ευθύνης των πλατφορμών και πώς αυτές τυχόν δύνανται να απαλλαχθούν ενώ, όπως και στις υπάρχουσες διαδικτυακές δραστηριότητες, πόσο μάλλον στο metaverse οι σχετικές προκλήσεις είναι ήδη αρκετές και μπορούν να επιδεινωθούν ακόμα περισσότερο στο metaverse λόγω του ότι ως πλατφόρμα «*βασίζεται σε αποκεντρωμένη και ανώνυμη τεχνολογία*»[223]. Μένει να αποδειχθεί το πώς πράγματι θα εφαρμοστεί στην πράξη η DSA και εντός του metaverse και τι συνέπειες μπορεί δυνητικά να ανακύψουν από την εν λόγω εφαρμογή. Σε κάθε δε περίπτωση υποστηρίζεται ότι στο metaverse ο έλεγχος του περιεχομένου, το οποίο προσπαθεί σε μεγάλο βαθμό να ρυθμίσει η DSA, θα πρέπει να είναι πολυδιάστατος λόγω και του πολυδιάστατου χαρακτήρα του metaverse και να μην περιορίζεται μόνο στο ίδιο το περιεχόμενο αλλά να συμπεριλαμβάνει και τη συμπεριφορά των ίδιων των άβαταρ[224].

[222] Maciejewski, M. (2023), ό.π., σελ. 116
[223] Europol (2022), ό.π., σελ. 21
[224] Boni, M. (2023), *Ethical challenges related to the Metaverse development -hypothesis, IntechOpen.* Διαθέσιμο σε: https://www.intechopen.com/online-first/1131705 (Τελευταία πρόσβαση: 16.06.2023)

5. METAVERSE ΚΑΙ ΖΗΤΗΜΑΤΑ ΑΝΤΑΓΩΝΙΣΜΟΥ

Με δεδομένο ότι το metaverse θα αποτελείται από επιμέρους metaverses και άρα στο πλαίσιο αυτό ενδέχεται να υπάρχουν αρκετοί πάροχοι των επιμέρους πλατφορμών για τις υπηρεσίες του metaverse, ενδέχεται να τεθούν κάποια ουσιώδη ζητήματα που να δημιουργούν προκλήσεις στο πλαίσιο του ανταγωνισμού. Αρκετές μεγάλες εταιρείες που δραστηριοποιούνται στον τομέα της τεχνολογίας, επεκτείνουν τη δραστηριοποίησή τους στο metaverse π.χ. μέσω εξαγορών ή συγχωνεύσεων, με αποτέλεσμα να δημιουργούνται ήδη ερωτήματα σχετικά με την εφαρμογή των σχετικών κανόνων ανταγωνισμού και εξαγορών ή συγχωνεύσεων προκειμένου να διαμορφωθούν τα δομικά στοιχεία του περιβάλλοντος του metaverse[225].

Όπως είναι ήδη γνωστό, η εταιρεία Meta είναι μία από τις εταιρείες, οι οποίες επενδύουν στον τομέα του metaverse, ωστόσο σε τεχνικό επίπεδο δεν αρκεί μία μόνο εταιρεία που να μπορεί να υποστηρίξει το metaverse, καθώς απαιτείται «*ισχυρό υπολογιστικό σύστημα*»[226], το οποίο σήμερα δεν μπορεί να το υποστηρίξει μόνο μία εταιρεία και ως εκ τούτου είναι αναγκαία η συνεργασία μεταξύ περισσότερων εταιρειών και οργανισμών προκειμένου να υποστηριχθούν οι ελάχιστες απαιτήσεις λειτουργίας του metaverse. Ο δε Zuckerberg, ωστόσο, ενώ έχει αναφέρει ότι το όραμα της Meta είναι να μη συνιστά το metaverse προϊόν μίας και μόνο εταιρείας αλλά να επηρεάζει θετικά και να εμπλέκεται ολόκληρη η βιομηχανία, ήδη με τη μετονομασία της εταιρείας του σε Meta φαίνεται να επιθυμεί να έχει ο ίδιος το προβάδισμα, ίσως με το να σηματοδοτεί ότι η Meta είναι το συνώνυμο του metaverse σε αντιστοιχία *με τον όρο "Google" που πλέον αποτελεί το «συνώνυμο της αναζήτησης στο διαδίκτυο»*[227] με ό,τι επιδράσεις μπορεί να έχει μελλοντικά η συγκεκριμένη τάση της εν λόγω εταιρείας στο πεδίο του ανταγωνισμού.

Στο πλαίσιο αυτό, όπου η οργάνωση του περιβάλλοντος του metaverse χρειάζεται τη διασύνδεση και τη διαλειτουργικότητα πολλών επιμέρους πλατφορμών με ενδεχόμενο κίνδυνο την κυριαρχία λίγων και μεγάλων εταιρειών[228] αναδεικνύεται το πόσο σημαντικό είναι να ληφθούν υπόψιν πτυχές του δικαίου του ανταγωνισμού, ώστε να λειτουργεί το

[225] Madiega, T., Car, P. et aI., (2022), ό.π., σελ. 3-4
[226] Αποστολάτου, Χ. (2022), ό.π. σελ. 73
[227] Gorichanaz, T. (2022), ό.π., σελ.655
[228] Madiega, T., Car, P. et aI., (2022), ό.π., σελ. 3-4

metaverse δίχως να παραβιάζονται από τις εταιρείες παρόχους βασικές αρχές του ελεύθερου ανταγωνισμού.

5.1. Σύγχρονες προκλήσεις του metaverse στον τομέα του ανταγωνισμού

Καταρχάς, το πόσο σημαντική είναι η σύνδεση μεταξύ του metaverse και του δικαίου του ανταγωνισμού αναδεικνύεται ήδη σε ευρωπαϊκό επίπεδο καθώς τον Ιανουάριο του 2022, η Εκτελεστική Αντιπρόεδρος της Ευρωπαϊκής Επιτροπής και αρμόδια Επίτροπος για θέματα Ανταγωνισμού, Μαργκρέτε Βεστάγκερ επεσήμανε στην Politico, ότι ήδη η ομάδα της έχει εστιάσει τόσο στο metaverse όσο και στην τεχνητή νοημοσύνη προκειμένου να αντιμετωπιστούν οποιεσδήποτε καταστάσεις δημιουργίας αθέμιτου ανταγωνισμού, ενώ οι ρυθμιστικές αρχές ήδη μελετούν τυχόν δυσμενείς συνέπειες της τεχνητής νοημοσύνης και του ChatGPT στην εργασιακή αγορά. Στην εν λόγω συνέντευξή της η Βεστάγκερ υπογράμμισε ότι το metaverse λόγω του ότι θα εμφανίσει νέες αγορές και επιχειρήσεις, θα μπορεί να δημιουργήσει το πρόσφορο έδαφος για ύπαρξη δεσπόζουσας θέσης[229] και στο πλαίσιο αυτό θα ήταν ορθό να υφίσταται η κατάλληλη προετοιμασία και τυχόν νομοθετικές προβλέψεις για τις εν λόγω αλλαγές. Το Μάρτιο του 2023 σε ομιλία της επεσήμανε δε ότι είναι «*ήδη καιρός να ληφθεί υπόψιν το πώς οφείλει να είναι ο υγιής ανταγωνισμός εντός του metaverse*»[230].

Η εν λόγω έκκληση για δράση της Βεστάγκερ είναι πρωτοπόρος αναφορικά με την αναγκαιότητα του πώς θα επιβληθεί μελλοντικά η νομοθεσία του ανταγωνισμού στο metaverse, μια κατάσταση, η οποία δημιουργεί μια σειρά προκλήσεων και ερωτημάτων. Ενδεικτικά τίθεται το ερώτημα του πώς θα εγκλιματιστούν και θα συνεργαστούν οι αρχές επιβολής του δικαίου περί ανταγωνισμού σε διασυνδεδεμένα περιβάλλοντα, όπως είναι το metaverse καθώς και σε ποια χρονική στιγμή ακριβώς θα πρέπει να παρέμβουν, δίχως από τη μία πλευρά να επηρεάζουν την καινοτομία με την πρώιμη παρέμβαση τους και δίχως από την άλλη πλευρά να καθυστερήσουν σε τέτοιο βαθμό, ούτως ώστε να έχει ήδη επηρεαστεί

[229] Stolton, S. (2022), 'Vestager: Metaverse poses new competition challenges', *Politico*, 18 January. Διαθέσιμο σε: https://www.politico.eu/article/metaverse-new-competition-challenges-margrethe-vestager/ (Τελευταία πρόσβαση: 14.06.2023)

[230] Ευρωπαϊκή Επιτροπή (2023), *Keynote delivered by EVP Vestager for the Keystone Conference: A Triple Shift for competition policy*. Διαθέσιμο σε: https://ec.europa.eu/commission/presscorner/detail/el/SPEECH_23_1342 (Τελευταία πρόσβαση: 16.06.2023)

δυσμενώς η αγορά, να έχει ουσιωδώς στρεβλωθεί ο ανταγωνισμός και να υπάρχει μονοπώλιο καθώς και επικράτηση των μεγάλων εταιρειών «παιχτών» της αγοράς. Άλλωστε, λόγω της ταχείας εξέλιξης της τεχνολογίας, υφίσταται ο κίνδυνος και στην περίπτωση του metaverse, οι νομοθέτες να βρίσκονται ένα βήμα πίσω από τις εξελίξεις, κάτι το οποίο δημιουργεί το εύλογο ερώτημα περί του αν τα υπάρχοντα εργαλεία στο πεδίο του ανταγωνισμού θα είναι επαρκή να αντιμετωπίσουν τις σχετικές προκλήσεις ή θα αποδειχθούν αναποτελεσματικά[231].

Στο πλαίσιο αυτό, είναι πολύ σημαντικός ο ορισμός της σχετικής αγοράς, «*η οποία περιλαμβάνει όσα προϊόντα ή/και υπηρεσίες θεωρούνται εναλλάξιμα ή υποκατάστατα με κριτήριο τα χαρακτηριστικά τους, την τιμή και τη χρήση τους*»[232]. Ο προσδιορισμός της σχετικής αγοράς είναι ιδιαίτερα σημαντικός προκειμένου να διαπιστωθεί η ύπαρξη και εν συνεχεία κατάχρηση δεσπόζουσας θέσης. Ωστόσο, ο ακριβής καθορισμός της σχετικής αγοράς είναι δυσχερής όταν πρόκειται για ψηφιακά περιβάλλοντα, τα οποία δεν έχουν σύνορα και γεωγραφικά όρια. Στο δε metaverse δύο σενάρια δυνητικά θα μπορούσαν να καλύψουν την έννοια της σχετικής αγοράς. Πρώτον, θα μπορούσε να θεωρηθεί ως σχετική αγορά η καθαυτή υποδομή του metaverse και δεύτερον, εφόσον υπάρχουν πράγματι περισσότερες της μίας επιχειρήσεις που παρέχουν τις επιμέρους υποδομές του metaverse, τότε θα υφίστανται επιμέρους σχετικές αγορές εντός του metaverse π.χ. η σχετική αγορά της πώλησης ρούχων για τους χρήστες – άβαταρ[233]. Είναι, επίσης, κρίσιμο να υπάρξει γεωγραφική οριοθέτηση της αγοράς (γεωγραφική αγορά), η οποία ορίζεται ως «*το έδαφος στο οποίο όλες οι επιχειρήσεις βρίσκονται σε παρεμφερείς ή επαρκώς ομοιογενείς συνθήκες ανταγωνισμού, όσον αφορά ακριβώς τα οικεία προϊόντα ή υπηρεσίες*»[234]. Ο καθορισμός της γεωγραφικής αγοράς θα πρέπει, μεταξύ άλλων, να απεικονίζει τους κύριους παράγοντες της αγοράς, οι οποίοι αναμένεται ότι θα περιστείλουν την ανταγωνιστική συμπεριφορά και

---

[231] Mackenzie, R. et al., (2022), 'Legal issues (part 2) Managing antitrust & competition risk', *The Reed Smith Guide to the Metaverse - 2nd Edition.* Διαθέσιμο σε: https://www.reedsmith.com/en/perspectives/metaverse/2022/08/managing-antitrust-and-competition-risk (Τελευταία πρόσβαση: 16.06.2023)

[232] Megale, L. (2022). '(Meta)verse as the Next Escaper from Competition Public Enforcement'. *Market and Competition Law Review*, 6(2), 15-50. Διαθέσιμο σε: https://revistas.ucp.pt/index.php/mclawreview/article/view/11715 (Τελευταία πρόσβαση: 17.06.2023), σελ.24

[233] Megale, L. (2022), ό.π.

[234] Σπηλιόπουλος, Ο. (2020) *Οικονομικό δίκαιο της Ευρωπαϊκής Ένωσης*, Αθήνα – Θεσσαλονίκη: Εκδόσεις Σάκκουλα, σελ. 526

ως εκ τούτου το πρώτο ως άνω σενάριο φαίνεται ως η πιο εύκολη λύση στον καθορισμό των μεριδίων της αγοράς[235].

Ιδίως αναφορικά με το ζήτημα της συνεργασίας μεταξύ περισσότερων εταιρειών προκειμένου να πληρούνται οι βασικές απαιτήσεις λειτουργίας του παγκόσμιου και διαλειτουργικού metaverse καθώς και προκειμένου να παρέχεται ποικιλία επιλογών και βελτιωμένη εμπειρία στους χρήστες, σημειώνεται ότι καταρχήν η εν λόγω συνεργασία μεταξύ ανταγωνιστικών επιχειρήσεων που δραστηριοποιούνται στο metaverse φαίνεται θετική εξ απόψεως ανταγωνισμού[236]. Εφόσον λοιπόν πράγματι το ενιαίο metaverse θα υφίσταται κατόπιν συνεργασίας περισσοτέρων οντοτήτων προκειμένου να πραγματοποιείται με ορθό τρόπο η διαλειτουργικότητα των επιμέρους metaverses, είναι αναγκαία η ύπαρξη κάποιων βιομηχανικών προτύπων διαλειτουργικότητας. Ωστόσο, ο καθορισμός των προτύπων μπορεί να δημιουργήσει ζητήματα στον τομέα του ανταγωνισμού, τόσο αναφορικά με την ορθή και αμερόληπτη διαδικασία καθορισμού των εν λόγω προτύπων όσο και με τις εκάστοτε σχετικές συμφωνίες συνεργασίας με εμφανή τον κίνδυνο του περιορισμού της παραγωγής[237]. Ειδικότερα, οι μεγάλες εταιρείες τεχνολογίας μπορεί να καθορίσουν τα εν λόγω τεχνικά πρότυπα και πρωτόκολλα με τρόπο που να ευνοεί ή έστω να μην επηρεάζει δυσμενώς τις επιχειρηματικές τους πρακτικές αλλά τουναντίον με δυσμενείς επιπτώσεις για τους προγραμματιστές αλλά και τους καταναλωτές, οι οποίοι θα διαθέτουν περιορισμένες επιλογές[238].

Τα προβλήματα εντείνονται, όταν επί παραδείγματι, οι εν λόγω ανταγωνιστικές εταιρείες ανταλλάσσουν ευαίσθητες πληροφορίες στο πλαίσιο του ανταγωνισμού π.χ. για την τιμολόγηση των προϊόντων τόσο εντός του metaverse όσο και του φυσικού κόσμου[239] ή καταλήγουν σε συμφωνίες, οι οποίες θα οδηγούσαν στον καθορισμό τιμών της αγοράς ή κατανομής αυτής (καρτέλ) και με αυτόν τον τρόπο τίθενται ζητήματα παραβίασης του ανταγωνισμού. Η δε καινοτομία των ανταγωνιστών μπορεί να επηρεαστεί μέσω των λεγόμενων «*φονικών εξαγορών*», ήτοι εξαγορών εκ μέρους μεγάλων εταιρειών τυχόν μικρότερων εκκολαπτόμενων καινοτόμων ανταγωνιστικών εταιρειών με αποκλειστικό ή κύριο σκοπό τον πλήρη περιορισμό της ανάπτυξης και της καινοτομίας τους καθώς και της

[235] Megale, L. (2022), ό.π.
[236] Murphy, S. et aI., (2021), ό.π.
[237] Gordon, M. (2022), ό.π., σελ.4
[238] Madiega, T., Car, P. et aI., (2022), ό.π., σελ. 3-4
[239] Stolton, S. (2022), ό.π.

πρόληψης του μελλοντικού ανταγωνισμού[240]. Αξίζει να σημειωθεί ότι γενικότερα δεν ελέγχονται όλες οι εξαγορές και συγχωνεύσεις από τις αρχές, αλλά η κοινοποίηση γίνεται κυρίως όταν επιτευχθούν συγκεκριμένα όρια κύκλου εργασιών[241]. Επομένως, μέσω των εν λόγων συμπεριφορών οι εν λόγω εταιρείες παραβιάζουν τη νομοθεσία περί ανταγωνισμού καθώς και την αντιμονοπωλιακή νομοθεσία του πραγματικού κόσμου με τις κυρώσεις που προβλέπονται εκάστοτε[242]. Συνεπώς, οι μεγάλες εταιρείες τεχνολογίας (Big Tech), θα βρεθούν αντιμέτωπες με πρόσθετους ελέγχους για τυχόν παραβιάσεις της νομοθεσίας περί του ανταγωνισμού και της αντιμονοπωλιακής νομοθεσίας[243].

Ως εκ τούτου, οριζόντιες συμπράξεις, όπως το καρτέλ απαγορεύονται και στο πλαίσιο των εταιρειών που δραστηριοποιούνται στο metaverse, οι οποίες πρέπει να συμμορφώνονται με το άρθρο 101 της ΣΛΕΕ, το οποίο προβλέπει, μεταξύ άλλων, ότι «*είναι ασυμβίβαστες με την εσωτερική αγορά και απαγορεύονται όλες οι συμφωνίες μεταξύ επιχειρήσεων, όλες οι αποφάσεις ενώσεων επιχειρήσεων και κάθε εναρμονισμένη πρακτική, που δύνανται να επηρεάσουν το εμπόριο μεταξύ κρατών μελών και που έχουν ως αντικείμενο ή ως αποτέλεσμα την παρεμπόδιση, τον περιορισμό ή τη νόθευση του ανταγωνισμού εντός της εσωτερικής αγοράς, και ιδίως εκείνες οι οποίες συνίστανται: α) στον άμεσο ή έμμεσο καθορισμό των τιμών αγοράς ή πωλήσεως ή άλλων όρων συναλλαγής,· β) στον περιορισμό ή στον έλεγχο της παραγωγής, της διαθέσεως, της τεχνολογικής αναπτύξεως ή των επενδύσεων, γ) στην κατανομή των αγορών ή των πηγών εφοδιασμού,· δ) στην εφαρμογή ανίσων όρων επί ισοδυνάμων παροχών, έναντι των εμπορικώς συναλλασσομένων, με αποτέλεσμα να περιέρχονται αυτοί σε μειονεκτική θέση στον ανταγωνισμό, ε) στην εξάρτηση της συνάψεως συμβάσεων από την αποδοχή, εκ μέρους των συναλλασσομένων, προσθέτων παροχών που εκ φύσεως ή σύμφωνα με τις εμπορικές συνήθειες δεν έχουν σχέση με το αντικείμενο των συμβάσεων αυτών*»[244]. Αντίστοιχη πρόβλεψη έχει υιοθετηθεί στην ελληνική έννομη τάξη με το άρθρο 1 (απαγορευμένες συμπράξεις) του Ν.3959/2011 περί προστασίας του ελεύθερου ανταγωνισμού.

---

[240] Madiega, T., Car, P. et al., (2022), ό.π., σελ. 4
[241] Megale, L. (2022), ό.π., σελ. 31-32
[242] Murphy, S. et al., (2021), ό.π.
[243] Gordon, M. (2022), σελ. 4
[244] *Ενοποιημένη απόδοση της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης Πρωτόκολλα Παραρτήματα της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης Δηλώσεις οι οποίες προσαρτώνται στην τελική πράξη της διακυβερνητικής διάσκεψης η οποία υιοθέτησε τη Συνθήκη της Λισσαβώνας που υπογράφηκε στις 13 Δεκεμβρίου 2007.* Διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A12016ME%2FTXT (Τελευταία πρόσβαση: 16.06.2023)

Περαιτέρω, εντός του metaverse θα τεθούν πιθανότατα και ζητήματα δεσπόζουσας θέσης και δη κατάχρηση της. Ήδη ορισμένες ρυθμιστικές αρχές, όπως η γερμανική αρχή ανταγωνισμού Bundeskartellamt, αντιμετωπίζουν ζητήματα περί των δεσποζουσών θέσεων στην ανερχόμενη αγορά εικονικής πραγματικότητας[245], όπως συνέβη σε υπόθεση σχετικά με την τεχνολογία VR της Oculus, η οποία είναι θυγατρική της Meta και ως συνέπεια της οποίας αποσύρθηκαν τα σχετικά προϊόντα της από τη Γερμανία. Στην εν λόγω υπόθεση, η Bundeskartellamt έλεγξε αν η Oculus καταστρατηγεί, τόσο τις διατάξεις περί προσωπικών δεδομένων, όσο και τις διατάξεις περί δικαίου του ανταγωνισμού καθώς στην εν λόγω υπόθεση προκειμένου να γίνει χρήση του hardware, έπρεπε να υπάρξει «*διασύνδεση ενός λογαριασμού Oculus με έναν λογαριασμό Facebook*»[246]. Προκύπτει, συνεπώς, και από αντίστοιχα περιστατικά ότι η δομή του metaverse παρέχει στις μεγάλες εταιρείες τεχνολογίας τη δυνατότητα μονοπώλησης των ψηφιακών αγορών, ήτοι οι ίδιες εταιρείες που είναι κυρίαρχες τη σημερινή εποχή στις ψηφιακές αγορές, οι ίδιες θα επιδιώξουν αντίστοιχη κυριαρχία στο metaverse δημιουργώντας ζητήματα ανταγωνισμού, τα οποία μπορούν, μεταξύ άλλων, να οδηγήσουν σε κατάχρηση της δεσπόζουσας θέσης τους π.χ. διατήρηση υπαρχουσών αντιανταγωνιστικών συμπεριφορών όπως π.χ. οι πρακτικές συστηματικής αυτοπροτίμησης, ήτοι η προτίμηση των δικών τους προϊόντων[247].

Επομένως και εντός του metaverse δύνανται να τεθούν ζητήματα κατάχρησης δεσπόζουσας θέσης και άρα θα πρέπει οι επιχειρήσεις να είναι ιδιαιτέρως προσεχτικές με τις σχετικές συμπεριφορές τους καθώς θα μπορούσε να τύχει εφαρμογής και εντός της δραστηριοποίησης στο χώρο του metaverse το άρθρο 102 ΣΛΕΕ, αντίστοιχη ρύθμιση στην ελληνική έννομη τάξη προβλέπεται στο άρθρο 2 του Ν.3959/2011. Σύμφωνα με το άρθρο 102 ΣΛΕΕ, «*είναι ασυμβίβαστη με την εσωτερική αγορά και απαγορεύεται, κατά το μέτρο που δύναται να επηρεάσει το εμπόριο μεταξύ κρατών μελών, η καταχρηστική εκμετάλλευση από μία ή περισσότερες επιχειρήσεις της δεσπόζουσας θέσης τους εντός της εσωτερικής αγοράς ή σημαντικού τμήματός της. Η κατάχρηση αυτή δύναται να συνίσταται ιδίως: α) στην άμεση ή έμμεση επιβολή μη δικαίων τιμών αγοράς ή πωλήσεως ή άλλων όρων συναλλαγής, β) στον περιορισμό της παραγωγής, της διαθέσεως ή της τεχνολογικής αναπτύξεως επί ζημία των καταναλωτών, γ) στην εφαρμογή άνισων όρων επί ισοδυνάμων παροχών έναντι των εμπορικώς*

[245] Madiega, T., Car, P. et aI., (2022), ό.π., σελ. 4
[246] Αποστολάτου, Χ. (2022), ό.π. σελ. 63
[247] Madiega, T., Car, P. et aI., (2022), ό.π., σελ. 4

συναλλασσομένων, με αποτέλεσμα να περιέρχονται αυτοί σε μειονεκτική θέση στον ανταγωνισμό, δ) στην εξάρτηση της συνάψεως συμβάσεων από την αποδοχή, εκ μέρους των συναλλασσομένων, προσθέτων παροχών που εκ φύσεως ή σύμφωνα με τις εμπορικές συνήθειες δεν έχουν σχέση με το αντικείμενο των συμβάσεων αυτών»[248]. Επομένως, οι εν λόγω συμπεριφορές που οδηγούν σε κατάχρηση δεσπόζουσας θέσης πρέπει να απαγορεύονται και εντός του metaverse.

Περαιτέρω εμπόδια μπορεί να εμφανιστούν στον τρόπο με τον οποίο οι αρμόδιες αρχές θα έχουν τα κατάλληλα μέσα για να ελέγξουν ένα πλήρως εικονικό περιβάλλον και συνεπώς κρίνεται αναγκαία η ύπαρξη εργαλείων, τα οποία θα μπορούν να ελέγχουν τον πηγαίο κώδικα του λογισμικού, ο οποίος πιθανότατα θα είναι η πηγή των συμπαιγνιακών συμπεριφορών ή συμπεριφορών αποκλεισμού εις βάρος άλλων ανταγωνιστών[249]. Άλλο ένα ζήτημα, το οποίο θα μπορούσε να επιδράσει στον ανταγωνισμό σχετίζεται με το σύνολο των δεδομένων που δύναται να υφίστανται σε μία διαδικτυακή πλατφόρμα, καθώς όσα περισσότερα δεδομένα κατέχει τόσο αυξάνεται η αξία της ενώ γίνεται πάρα πολύ δύσκολο για έναν άλλο ανταγωνιστή να ανέλθει στην κατοχή ίδιου βαθμού συνόλου δεδομένων και ως εκ τούτου θα μπορούσε να αποκλειστεί από την εν λόγω αγορά[250].

Προκειμένου να μετριαστούν οι ανωτέρω κίνδυνοι θα πρέπει να ληφθεί μια σειρά μέτρων, τόσο εκ μέρους των επιχειρήσεων όσο και εκ μέρους των αρμόδιων αρχών. Η εκ των προτέρων συνεργασία τόσο μεταξύ των ρυθμιστικών αρχών όσο και των μεγάλων «παικτών» κρίνεται ουσιώδης προκειμένου να αναπτυχθεί το metaverse με τρόπο κατά τον οποίο να διασφαλίζεται ότι είναι ανοικτό με την έννοια της πρόσβασης των ανταγωνιστών[251]. Οι δε επιχειρήσεις που δραστηριοποιούνται στο metaverse θα πρέπει να υιοθετήσουν πολιτικές στο πεδίο του ανταγωνισμού[252].

Περαιτέρω, οι αρμόδιες αρχές ανταγωνισμού θα πρέπει καταρχάς να διασφαλίσουν ότι εποπτεύουν επαρκώς και καταλλήλως το metaverse διασφαλίζοντας ότι αναπτύσσεται ένα περιβάλλον με προϊόντα και υπηρεσίες, το οποίο είναι ανοιχτό στην πρόσβαση άλλων

---

[248] *Ενοποιημένη απόδοση της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης Πρωτόκολλα Παραρτήματα της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης Δηλώσεις οι οποίες προσαρτώνται στην τελική πράξη της διακυβερνητικής διάσκεψη η οποία υιοθέτησε τη Συνθήκη της Λισσαβώνας που υπογράφηκε στις 13 Δεκεμβρίου 2007, ό.π.*

[249] Stolton, S. (2022), ό.π.

[250] Megale, L. (2022), ό.π., σελ. 36

[251] Megale, L. (2022), ό.π., σελ. 28

[252] Murphy, S. et aI., (2021), ό.π.

ανταγωνιστών και στο πλαίσιο αυτό θα μπορούσαν να συσταθούν εσωτερικοί μηχανισμοί αξιολόγησης, οι οποίοι θα αντιμετώπιζαν με αυτόματο τρόπο ζητήματα στον πηγαίο κώδικα του metaverse[253].

Εξίσου σημαντικό ρόλο κατέχει η εκ των προτέρων ρύθμιση και έλεγχος των συγκεντρώσεων. Η εκ των προτέρων ρύθμιση είναι προτιμότερη με την έννοια ότι προλαμβάνει τη βλάβη στο πλαίσιο του ανταγωνισμού πριν τούτη επέλθει, έχει δηλαδή προληπτική λειτουργία σε αντίθεση με την εκ των υστέρων ρύθμιση, η οποία είναι χρονοβόρα και ανεπαρκής ιδίως στο πλαίσιο του ψηφιακού τομέα, ο οποίος εξελίσσεται διαρκώς. Θα πρέπει περαιτέρω, οι αρμόδιες αρχές να αναπτύξουν τα κατάλληλα εργαλεία, τα οποία θα ελέγχουν τις συγχωνεύσεις και εξαγορές πριν αυτές πραγματοποιηθούν και να αποδυναμώνουν τέτοιου είδους ενέργειες, όταν πρόκειται να επηρεαστεί δυσμενώς ο ανταγωνισμός εντός του metaverse και παράλληλα να διαφυλαχθεί ότι οι αγορές στο metaverse παραμένουν ανοικτές και ελεύθερες[254].

Άλλωστε ως ένα εργαλείο μεταξύ των αρχών και των επιχειρήσεων θα μπορούσαν να χρησιμοποιηθούν οι έξυπνες συμβάσεις (smart contracts), μέσω των οποίων θα μπορούσε να διαπιστωθεί αν μια επιχείρηση που έχει προηγουμένως δεσμευτεί στη μη αύξηση ή στη μείωση των τιμών σε ορισμένο ποσοστό, παραβιάζει την εν λόγω δέσμευση και κατ' αποτέλεσμα επέρχονται οι αντίστοιχες καθορισμένες συνέπειες[255].

Αναφορικά με το ζήτημα των συγχωνεύσεων και εξαγορών, το βασικότερο ζήτημα είναι ότι δεν υφίσταται ομοιόμορφη προσέγγιση μεταξύ των διαφόρων κρατών μελών της Ε.Ε., κάτι το οποίο οδηγεί σε ανασφάλεια επί του ζητήματος και επιδρά δυσμενώς στις εξαγορές. Στο πλαίσιο αυτό, η αξιολόγηση των συγχωνεύσεων και εξαγορών εκ μέρους των αρχών κρίνεται μεν ουσιώδης αλλά μια διεθνής ρυθμιστική συνεργασία[256] θα ήταν η κατάλληλη για την επίλυση του εν λόγω ζητήματος σε περιβάλλοντα, όπως το metaverse.

Επιπροσθέτως, κρίσιμο στοιχείο είναι να θεωρηθεί η διαλειτουργικότητα και ως απαίτηση στο πλαίσιο του πεδίου του ανταγωνισμού, ήτοι οι ψηφιακές πλατφόρμες να οφείλουν να δίδουν στους καταναλωτές - χρήστες τη δυνατότητα να μεταφέρουν τα δεδομένα τους ακόμη και σε ανταγωνιστική πλατφόρμα κατά τη στιγμή που αποφασίζουν να αποχωρήσουν από την εκάστοτε πλατφόρμα. Σε διαφορετική περίπτωση, θα υφίσταται

[253] Megale, L. (2022), ό.π., σελ. 43
[254] Mackenzie, R. et al., (2022), ό.π.
[255] Megale, L. (2022), ό.π., σελ. 45
[256] Megale, L. (2022), ό.π., σελ. 44

ο κίνδυνος να αποκτήσει υπέρμετρη ισχύ εις βάρος των υπολοίπων μια ψηφιακή πλατφόρμα, η οποία εγκλωβίζει τους καταναλωτές της σε αυτή, υπό την έννοια ότι αν αποχωρήσουν οι χρήστες θα απωλέσουν τα δεδομένα τους και κατά συνέπεια δεν θα υφίσταται πράγματι διαλειτουργικότητα μεταξύ των πλατφορμών[257].

5.2. Ειδικότερα η DMA στο metaverse

Πέρα από την εφαρμογή της DSA, η οποία αναφέρθηκε ανωτέρω και καλείται να συνδράμει σε ζητήματα περί της ευθύνης εντός του metaverse, στο πλαίσιο του ανταγωνισμού εξ αφορμής του metaverse είναι καίρια η εφαρμογή της DMA, η οποία σε συνδυασμό με τη DSA στοχεύει στην εναρμόνιση της εσωτερικής αγοράς και στην αποτροπή των «*τεχνολογικών γιγάντων*»[258] από το να καταλάβουν τούτοι δεσπόζουσα θέση στον τομέα των ψηφιακών υπηρεσιών. Σύμφωνα με τη Βεστάγκερ, επί του παρόντος, δεν υπάρχει η βούληση εκ μέρους της Ευρωπαϊκής Επιτροπής να προσθέσει ειδικότερες προβλέψεις για το metaverse στις DSA και DMA[259]. Σημειωτέον ότι η DMA καλείται να συμπληρώσει την ισχύουσα νομοθεσία περί προστασίας του ανταγωνισμού τόσο σε επίπεδο Ε.Ε. όσο και σε εθνικό επίπεδο[260] δίχως να θίγει την εφαρμογή των άρθρων 101 και 102 ΣΛΕΕ και αντίστοιχων εθνικών κανόνων ανταγωνισμού, σύμφωνα και με το άρθρο 1 παρ. 6 της DMA.

Η DMA εφαρμόζεται, ειδικότερα, σε αθέμιτες πρακτικές που προέρχονται από ρυθμιστές πρόσβασης, οι οποίες, είτε δεν εντάσσονται στους υπάρχοντες ενωσιακούς κανόνες περί του ελέγχου του ανταγωνισμού, είτε δεν ρυθμίζονται σε αποτελεσματικό βαθμό από τους ως άνω κανόνες λόγω του ότι οι εν λόγω κανόνες τίθενται σε εφαρμογή εκ των υστέρων και ανά περίπτωση και συνεπώς η DMA καλείται να δράσει εκ των προτέρων και να προλάβει τις δυσμενείς επιπτώσεις τέτοιου είδους πρακτικών συνεπικουρώντας την εκ των υστέρων εφαρμογή των υπαρχόντων ενωσιακών κανόνων ανταγωνισμού[261]. Η DMA

---

[257] Mackenzie, R. et al., (2022), ό.π.

[258] Angeles, J. (2022), ό.π., σελ. 297

[259] Council of the European Union (2022), Metaverse – Virtual World, Real Challenges. Διαθέσιμο σε: https://www.consilium.europa.eu/media/54987/metaverse-paper-9-march-2022.pdf (Τελευταία πρόσβαση: 17.06.2023), σελ. 12

[260] Ευρωπαϊκή Επιτροπή (2023), *Ερωτήσεις και απαντήσεις: Πράξη για τις ψηφιακές αγορές: Διασφάλιση δίκαιων και ανοικτών ψηφιακών αγορών.* Διαθέσιμο σε: https://ec.europa.eu/commission/presscorner/detail/el/QANDA_20_2349 (Τελευταία πρόσβαση: 17.06.2023)

[261] Ευρωπαϊκή Επιτροπή (2023), *Ερωτήσεις και απαντήσεις: Πράξη για τις ψηφιακές αγορές: Διασφάλιση δίκαιων και ανοικτών ψηφιακών αγορών*, ό.π.

στοχεύει να δημιουργήσει ισότιμους όρους ανταγωνισμού μεταξύ των πλατφορμών ρυθμιστών της πρόσβασης και λοιπών μικρότερων επιχειρήσεων και ως εκ τούτου ενδυναμώνεται η καινοτομία, βελτιώνεται η ποιότητα των υπηρεσιών και αυξάνεται η ευημερία των χρηστών - καταναλωτών[262].

Στο πλαίσιο αυτό, καθίσταται σαφές ότι τα κύρια ενδιαφερόμενα μέρη του metaverse ενδέχεται να θεωρηθούν ως πυλωροί – ρυθμιστές πρόσβασης[263], σύμφωνα με το άρθρο 3 της DMA, εφόσον πληρούνται οι προβλέψεις του εν λόγω άρθρου, ήτοι καταρχήν η εν λόγω επιχείρηση «*έχει σημαντικό αντίκτυπο στην εσωτερική αγορά, παρέχει βασική υπηρεσία πλατφόρμας, η οποία αποτελεί σημαντική πύλη για να συνδέονται οι επαγγελματίες χρήστες με τελικούς χρήστες, κατέχει παγιωμένη και σταθερή θέση, στο πλαίσιο των δραστηριοτήτων της, ή αναμένεται ότι θα κατέχει τέτοια θέση στο εγγύς μέλλον*». Εν προκειμένω, υφίστανται και τεκμήρια, τα οποία προβλέπονται στην παράγραφο 2 του άρθρου 3 της DMA και σηματοδοτούν την υπαγωγή μιας πλατφόρμας στην έννοια του ρυθμιστή πρόσβασης. Εφόσον, κάποια πλατφόρμα θεωρείται ότι υπάγεται στην έννοια του ρυθμιστή πρόσβασης, τότε υπόκειται σε συγκεκριμένες υποχρεώσεις και απαγορεύσεις π.χ. απαγόρευση διενέργειας αθέμιτων συμπεριφορών που πλήττουν τον ανταγωνισμό[264].

Η DMA σε αντιστοιχία με τη DSA προσπαθεί μεταξύ άλλων να ρυθμίσει τους Big Tech, κάτι το οποίο αναδεικνύεται και στα ως άνω τεκμήρια περί υπαγωγής μιας επιχείρησης στην έννοια του πυλωρού, ήτοι ένα εκ των τεκμηρίων αναφέρεται σε ετήσιο κύκλο εργασιών μιας επιχείρησης στην Ένωση ίσο ή μεγαλύτερο από 7,5 δισεκατομμύρια ευρώ. Και τούτο διότι οι εν λόγω επιχειρήσεις κατέχουν προνομιακή θέση στη ψηφιακή αγορά με κίνδυνο εξάλειψης κάθε πιθανού ανταγωνισμού και καινοτομίας εκ μέρους των μικρών και νέων επιχειρήσεων ιδίως, αν αναλογιστεί κανείς, επί παραδείγματι, τις συνεχείς εξαγορές στις οποίες προβαίνει κατά καιρούς η Meta. Ως εκ τούτου η DMA επιδιώκει να διασφαλίσει μια δικαιότερη ανοιχτή ψηφιακή αγορά θέτοντας τα εχέγγυα για έναν πιο υγιή ανταγωνισμό και άρα για ένα πιο υγιές metaverse[265].

---

[262] Ευρωπαϊκή Επιτροπή, *Μια Ευρώπη έτοιμη για την ψηφιακή εποχή: νέοι κανόνες για τις διαδικτυακές πλατφόρμες*, ό.π.

[263] Murphy, S. et aI., (2021), ό.π.

[264] Ευρωπαϊκή Επιτροπή (2023), *Ερωτήσεις και απαντήσεις: Πράξη για τις ψηφιακές αγορές: Διασφάλιση δίκαιων και ανοικτών ψηφιακών αγορών*, ό.π.

[265] Bravo, A. (2023). 'MDE#07 The Digital Markets Act'. Διαθέσιμο σε: https://www.metaversethics.org/p/mde07-the-digital-markets-act (Τελευταία πρόσβαση: 17.06.2023)

Με δεδομένο, επομένως, ότι το στοιχείο της διαλειτουργικότητας θα κυριαρχήσει κατά τη λειτουργία του metaverse, η DMA στοχεύει στην εξασφάλιση της ισορροπίας της αγοράς, με στόχο να αποφευχθεί μια μεμονωμένη εταιρεία να καταστεί ρυθμιστής της πρόσβασης με την έννοια ότι θα κατέχει προνομιακή θέση ή δεσπόζουσα θέση στη ψηφιακή αγορά[266]. Αξίζει να σημειωθεί ότι η DMA δεν περιέχει σημαντικές αλλαγές στον έλεγχο των συγκεντρώσεων. Ειδικότερα, στο άρθρο 14 της DMA περιέχεται πρόβλεψη περί της υποχρέωσης ενημέρωσης σχετικά με τις συγκεντρώσεις, η οποία συνιστά τρόπο ενημέρωσης της Επιτροπής σε πραγματικό χρόνο και πριν την πραγματοποίηση της συγκέντρωσης με δεδομένο ότι νομική βάση της DMA είναι η εσωτερική αγορά ενώ οι φονικές εξαγορές θα πρέπει να έχουν ως νομική βάση την κατάχρηση δεσπόζουσας θέσης σύμφωνα με το άρθρο 102 ΣΛΕΕ[267].

Ο βασικός προβληματισμός που ανακύπτει στο πλαίσιο αυτό, είναι η πρόβλεψη των μελλοντικών συνεπειών των εξαγορών καθώς και συγχωνεύσεων σε πτυχές του metaverse, οι οποίες δεν έχουν προβλεφθεί ακόμα με δεδομένη την ταχεία εξέλιξη τόσο των τεχνολογιών όσο και της καθαυτής αγοράς, με άμεση αναγκαιότητα των αρχών ανταγωνισμού να βρίσκονται σε εγρήγορση προκειμένου να εξετάζεται κατά πόσο μια επιχείρηση που, επί παραδείγματι, εξαγοράζεται σήμερα, θα αποτελούσε τον αυριανό ανταγωνιστή της επιχείρησης που την εξαγοράζει. Μια ακόμη πρόκληση συνίσταται στο γεγονός ότι εξαιτίας των ταχύτατων εξελίξεων στον ψηφιακό τομέα, τα όρια της αγοράς μπορούν να μεταβληθούν πολύ γρήγορα[268], επηρεάζοντας τα μέχρι τότε υφιστάμενα όρια.

[266] Angeles, J. (2022), ό.π., σελ. 298
[267] Megale, L. (2022), ό.π., σελ. 32-33
[268] Megale, L. (2022), ό.π., σελ. 32-33

6. METAVERSE ΚΑΙ ΑΣΦΑΛΕΙΑ

Η χρήση του metaverse και δη οι τεχνολογίες XR, AR, VR, θέτουν αντιμέτωπο το χρήστη με μια σειρά κινδύνων ασφαλείας. Πιο συγκεκριμένα, δύνανται να εκδηλωθούν σημαντικές καταστάσεις κυβερνοεπιθέσεων, ήτοι να προκύψουν ουσιώδη προβλήματα κυβερνοασφάλειας και παραβίασης των προσωπικών δεδομένων καθώς και να ανακύψουν περιστατικά διακύβευσης της ασφάλειας του ίδιου του χρήστη εντός του metaverse, ήτοι διάπραξης ποινικών αδικημάτων που θέτουν σε κίνδυνο την ασφάλεια του χρήστη. Μέσω της παρούσας, ο όρος της ασφάλειας στο metaverse θα εξεταστεί τόσο με την οπτική της κυβερνοασφάλειας όσο και με την οπτική της ουσιαστικής ασφάλειας του χρήστη στο περιβάλλον του metaverse εξ απόψεως των διαφόρων ποινικών αδικημάτων που μπορούν να λάβουν χώρα στο περιβάλλον του metaverse.

6.1. Metaverse και κυβερνοασφάλεια

Καταρχάς, εντός του metaverse οι κυβερνοεπιθέσεις και οι κίνδυνοι ασφαλείας θα «εξελιχθούν» υπό την έννοια ότι θα δύνανται να λάβουν διαφορετική μορφή και θα διαφέρουν από τις επιθέσεις και απειλές, όπως τούτες εμφανίζονται σήμερα στο διαδίκτυο. Επί παραδείγματι, δυνητικά θα μπορούσαν να υπάρξουν εντονότερα περιστατικά, τα οποία θα ήταν δυσκόλως ανιχνεύσιμα εις βάρος των χρηστών, ήτοι περιστατικά παράνομης πρόσβασης και υποκλοπής – το λεγόμενο hacking- μιας λόγου χάρη φωνητικής κλήσης ή με παράνομο τρόπο να υπάρξει πρόσβαση σε πλατφόρμα του metaverse καθώς και να δημιουργηθούν «*πλαστά ή χακαρισμένα αβαταρ*»[269]. Η τεράστια ποσότητα των δεδομένων που θα κυκλοφορούν στο metaverse καθώς και ο δυνητικός τρόπος χρήσης των εν λόγω δεδομένων εντείνουν τον κίνδυνο κυβερνοασφάλειας για τους χρήστες[270].

Παρά το γεγονός ότι το metaverse συνίσταται σε μια σειρά νέων και εξελιγμένων τεχνολογιών, πάντοτε οι δράστες θα εντοπίζουν νέους τρόπους επίθεσης στα ψηφιακά περιβάλλοντα και άρα δυνητικά και στο metaverse. Όπως και παλαιότερα που ήταν δύσκολο να εντοπιστεί ο τρόπος διάπραξης των εγκλημάτων του διαδικτύου, έτσι στην αρχή θα είναι δυσχερής και ο εντοπισμός του τρόπου διάπραξης των εγκλημάτων εντός του metaverse λόγω, μεταξύ άλλων, της πολυεπίπεδης δομής του εν λόγω εικονικού περιβάλλοντος, το

[269] Κόκιου, Β. (2022), ό.π.
[270] Madiega, T., Car, P. et aI., (2022), ό.π., σελ. 8

οποίο δυνητικά επιτρέπει στους δράστες «*να κρυφτούν πίσω από κρυπτογράφηση και μη ανιχνεύσιμα NFTs*»[271]. Σε αντιστοιχία με υπάρχουσες πλατφόρμες και συστήματα λογισμικού δύνανται να υπάρξουν και στο metaverse πολλές απειλές ασφαλείας, όπως ενδεικτικά, «*μη ασφαλής αρχιτεκτονική συστήματος, μη ενημερωμένο ή κακόβουλο λογισμικό, ransomware*»[272]. Εν προκειμένω, οι δράστες δύνανται να εκμεταλλευτούν τις όποιες αδυναμίες έχουν οι τεχνολογίες στις οποίες βασίζεται το metaverse π.χ. τις συσκευές που βασίζονται στην τεχνολογία XR.

Ειδικότερα, αξίζει να σημειωθεί ότι κάποιες συσκευές μπορούν να χρησιμοποιηθούν προκειμένου να πιστοποιηθεί η ταυτότητα του χρήστη χωρίς τη συμπλήρωση ονόματος χρήστη και κωδικού πρόσβασης προκειμένου να ελεγχθεί η πρόσβαση στο περιεχόμενο. Επιπρόσθετα, οι εν λόγω συσκευές συνδέονται με βιομετρικά δεδομένα π.χ. παρακολούθηση φυσικών κινήσεων, όπως έχει ήδη αναφερθεί. Οι ήδη υφιστάμενες προκλήσεις κυβερνοαφάλειας π.χ. phising, και hacking θα ενταθούν και θα επηρεάσουν και τις ίδιες τις συσκευές που προσφέρουν την εμπειρία του metaverse στους χρήστες[273]. Λαμβάνοντας υπόψιν τα ως άνω, οι κακόβουλοι επιτιθέμενοι εκμεταλλευόμενοι τα τρωτά σημεία ασφαλείας των εν λόγω συσκευών θα μπορούσαν παρανόμως να αποκτήσουν τα δικαιώματα του χρήστη της συσκευής και να προβούν σε έλεγχο των συσκευών εξ αποστάσεως[274], παραβιάζοντας την προστασία των προσωπικών δεδομένων διότι θα μπορούσαν να αποσπαστούν πληροφορίες που να σχετίζονται με ειδικές κατηγορίες προσωπικών δεδομένων που απαιτούνται για τη λειτουργία των εν λόγω συσκευών π.χ. πληροφορίες για το βλέμμα, κίνηση του προσώπου καθώς και παράνομη απόκτηση πληροφοριών σχετικά με τις δραστηριότητες του χρήση π.χ. μέσα στο σπίτι ή κατά την εργασία του, δηλαδή τι ακούει, τι βλέπει, τι κάνει ο χρήστης στον προσωπικό του χώρο[275].

Άλλωστε, είναι εφικτό οι δράστες να δύνανται να αποκτήσουν ευαίσθητες και σημαντικές πληροφορίες μέσω επιθέσεων sniffing ή spoofing στο metaverse καθώς είναι σύνηθες οι πλατφόρμες metaverse να μη διαθέτουν κρυπτογράφηση «*ούτε για τις συνδέσεις δικτύου, (ήτοι από τη συσκευή του χρήστη προς την πλατφόρμα) ούτε για τις συνδέσεις μεταξύ των άβαταρ*»[276]. Η δε τεχνολογία VR επιτρέπει στους δράστες να μπορούν να προβούν σε

[271] Madiega, T., Car, P. et aI., (2022), ό.π., σελ. 8
[272] Dwivedi, K. Y. et al. (2022), ό.π., σελ. 8
[273] Madiega, T., Car, P. et aI., (2022), ό.π., σελ. 8
[274] Dwivedi, K. Y. et al. (2022), ό.π., σελ. 8
[275] Madiega, T., Car, P. et aI., (2022), ό.π., σελ. 8
[276] Dwivedi, K. Y. et al. (2022), ό.π., σελ. 8

χειραγώγηση του συναισθήματος του θύματος με τρόπο που να μπορεί κάποιος χάκερ να έχει πρόσβαση και στο ψυχισμό και στο σώμα του θύματος[277].

Προβλήματα κυβερνοασφάλειας μπορεί να υπάρξουν και στα κύρια δομικά οικονομικά στοιχεία του metaverse, ήτοι κρυπτονομίσματα και NFTs, τα οποία βασίζονται στην τεχνολογία blockchain, η οποία ενδέχεται να είναι ευάλωτη σε επιθέσεις hacking[278] και να δημιουργηθούν «*ζητήματα πώλησης πλαστών NFTs, παράνομης χρήσης κρυπτονομισμάτων καθώς και ύπαρξης κακόβουλων έξυπνων συμβάσεων*»[279]. Αναφορικά ιδίως με τις επιθέσεις τύπου ransomware, τούτες μπορεί να είναι ιδιαίτερα επικίνδυνες στις τεχνολογικές συσκευές του metaverse καθώς κακόβουλοι επιτιθέμενοι θα μπορούσαν να καταστήσουν αδύνατη την πρόσβαση στα ψηφιακά περιουσιακά στοιχεία των χρηστών, τα οποία κατέχουν αυξημένη σημασία στο metaverse, κάνοντας κρυπτογράφηση των κλειδιών πρόσβασης. Επί παραδείγματι, η πλατφόρμα Roblox έχει δεχτεί κατά καιρούς επιθέσεις από χάκερς, οι οποίοι «μόλυναν» την εν λόγω πλατφόρμα με ransomware, απαιτώντας ταυτόχρονα εικονικά νομίσματα, τα λεγόμενα Robux και υποχρεώνοντας ταυτόχρονα τους χρήστες του παιχνιδιού σε άσεμνες ενέργειες[280]. Σε άλλες δε περιπτώσεις οι δράστες θα μπορούσαν να αποκτήσουν παράνομη πρόσβαση στα εν λόγω ψηφιακά περιουσιακά στοιχεία των χρηστών[281].

Περαιτέρω, λόγω της χρήσης των άβαταρ, μέσω των οποίων οι χρήστες καθίστανται ρεαλιστικοί και μόνιμοι, θα μπορούσαν να δοθούν ευκαιρίες σε δράστες να προβούν σε αντιγραφή της εν λόγω εμφάνισης των χρηστών, δηλαδή να εμφανιστεί το φαινόμενο deepfakes, ήτοι μια μορφή τεχνολογίας που κάνει χρήση βαθιάς μάθησης με σκοπό την αντικατάσταση της εμφάνισης ενός ατόμου με ένα άλλο σε βίντεο ή μέσα ενημέρωσης και η οποία πολλές φορές χρησιμοποιείται για λόγους χειραγώγησης των ατόμων[282]. Το εν λόγω φαινόμενο μπορεί να έχει δυσμενέστερη μορφή εντός του metaverse λόγω του ότι υφίσταται μαζική συλλογή λεπτομερών δεδομένων για ένα χρήστη, τα οποία θα μπορούσαν να συνδράμουν στην προσθήκη χαρακτηριστικών της συμπεριφοράς ενός ατόμου στα

[277] Madiega, T., Car, P. et aI., (2022), ό.π., σελ. 8
[278] Dwivedi, K. Y. et al. (2022), ό.π., σελ. 10
[279] Madiega, T., Car, P. et aI., (2022), ό.π., σελ. 8
[280] Dwivedi, K. Y. et al. (2022), ό.π., σελ. 8
[281] Petrányi, D., Horváth, K. and Domokos, M. (2022) 'Part 3 - Data protection challenges, the importance of cybersecurity, advertising regulation in the metaverse', ό.π.
[282] Maciejewski, M. (2023), ό.π., σελ. 45

deepfakes δημιουργώντας σύνθετες καταστάσεις, ιδίως σε επίπεδο κατάχρησης ταυτότητας και επηρεασμού των πράξεων ενός χρήστη[283].

Αντίστοιχα προβλήματα δύνανται να εμφανιστούν και στους νέους τρόπους αλληλεπίδρασης των χρηστών με το σύστημα ένταξης στο metaverse χρησιμοποιώντας διάφορους αισθητήρες, καθώς και η χρήση των βιομετρικών πληροφοριών που προδίδουν μια σειρά ουσιωδών δεδομένων για τους χρήστες δημιουργώντας τις κατάλληλες συνθήκες για τους δράστες προς υποκλοπή της ταυτότητας των χρηστών, τους οποίους με αυτόν τον τρόπο δύνανται να υποδύονται πειστικότερα[284]. Το δε άβαταρ δημιουργεί διάφορες πληροφορίες π.χ. μέσω της φωνής καθώς και περιεχόμενο, το οποίο μπορεί να διαρρεύσει ή να πλαστογραφηθεί ή να γίνει κατάχρηση των εν λόγω πληροφοριών ή ακόμη και αλλοίωση του ίδιου του άβαταρ[285].

Επομένως, τίθεται το εύλογο ερώτημα του ποιος κατέχει την εικονική ταυτότητα ενός χρήστη με δεδομένο ότι όσο περισσότερα δεδομένα (συμπεριλαμβανομένων τούτων που δημιουργούνται μέσω των διάφορων αλληλεπιδράσεων του χρήστη εντός του metaverse) και όσο περισσότερο προσεγγίζει και αντιπροσωπεύει το άβαταρ τον χρήστη που βρίσκεται πίσω από αυτό, τόσο περισσότερο δυσχερής είναι η απάντηση στο εν λόγω ερώτημα περί της κατοχής της ταυτότητας του εν λόγω πραγματικού χρήστη[286]. Κίνδυνοι, όπως η κλοπή ταυτότητας καθώς και αντιγραφής του ίδιου του άβαταρ θέτουν, μεταξύ άλλων, ζητήματα διαλειτουργικότητας[287]. Συνεπώς, εξαιτίας των εν λόγω κινδύνων, για τους οποίους σε μεγάλο βαθμό ευθύνεται η τρωτότητα των εν λόγω συστημάτων εξ απόψεως ασφαλείας, δημιουργείται μεγάλη ανασφάλεια στο θέμα της ταυτότητας του χρήστη με αποτέλεσμα τόσο τη χειραγώγηση των χρηστών όσο και τη δημιουργία κλίματος αβεβαιότητας σε ουσιώδη θέματα εμπιστοσύνης, καθώς οι χρήστες δεν θα είναι πάντοτε σε θέση να γνωρίζουν με ποιον πράγματι αλληλεπιδρούν στο metaverse[288].

Περαιτέρω, η ύπαρξη διαθεσιμότητας είναι ακόμη μια αναγκαία προϋπόθεση για την ορθή λειτουργία του metaverse λόγω του ότι μια ενδεχομένως διακοπή της σύνδεσης του δικτύου ή περιστατικά ασφαλείας όπως «*κατανεμημένη άρνηση παροχής υπηρεσιών (DDos) μπορεί να έχει πιο σημαντικές επιπτώσεις στο metaverse σε αντίθεση με τις ασύγχρονες*

[283] Europol (2022), ό.π., σελ. 14
[284] Europol (2022), ό.π., σελ. 13
[285] Dwivedi, K. Y. et al. (2022), ό.π., σελ. 8
[286] Europol (2022), ό.π., σελ. 14
[287] Madiega, T., Car, P. et al., (2022), ό.π., σελ. 9
[288] Europol (2022), ό.π., σελ. 13

διαδικτυακές υπηρεσίες»[289]. Επιπλέον, λόγω της δομής του metaverse (διαλειτουργικότητα), αρκετές κυβερνοεπιθέσεις που αρχικά εμφανίζονται σε μια πλατφόρμα του metaverse π.χ. πλατφόρμα παιχνιδιού, δύνανται να επεκταθούν και σε περισσότερες πλατφόρμες επηρεάζοντας με αυτό τον τρόπο περισσότερους χρήστες και κοινότητες, λόγω της δομής και λειτουργίας του metaverse, το οποίο αποτελείται από πληθώρα διασυνδέσεων μεταξύ κοινοτήτων και διαφόρων εφαρμογών. Άλλωστε, οι εν λόγω διασυνδέσεις οδηγούν σε περισσότερες διαπροσωπικές επικοινωνίες, έτσι ώστε αυξάνονται οι τρόποι μέσω των οποίων δύνανται να συλλεχθούν διάφορες πληροφορίες, οι οποίες αν χρησιμοποιηθούν με καταχρηστικό τρόπο, τούτο μπορεί να συνεπάγεται τη διάπραξη μιας σειράς εγκλημάτων στον κυβερνοχώρο[290].

Με δεδομένο ότι τα υπάρχοντα συστήματα ασφαλείας, τα μέτρα προστασίας καθώς και οι σχετικές πολιτικές διαχείρισης, φαίνονται ανεπαρκή ενόψει των κινδύνων ασφαλείας του metaverse θα πρέπει να τύχουν βελτιώσεων προκειμένου να συνάδουν με τα χαρακτηριστικά και ιδιοσυγκρασίες του metaverse. Περαιτέρω, προκειμένου να μην υφίσταται ή να μειωθεί η εμφάνιση των ανωτέρω προβλημάτων ασφαλείας και επομένως να παρέχονται οι διάφορες υπηρεσίες του metaverse με ασφαλή και αποτελεσματικό τρόπο πρέπει να ληφθεί μια σειρά μέτρων προστασίας της κυβερνοασφάλειας και της ιδιωτικής ζωής[291] προκειμένου τόσο οι χρήστες όσο και τα συστήματα να προστατεύονται επαρκώς από τις ευπάθειες του ίδιου του συστήματος. Επί παραδείγματι, αναγκαία κρίνεται η ύπαρξη μιας λεπτομερούς πολιτικής ελέγχου της ταυτότητας του χρήστη καθώς και ελέγχου της πρόσβασης σε προσωπικά δεδομένα αλλά και ύπαρξη μέτρων ψευδωνυμοποίησης. Είναι ιδιαιτέρως σημαντικό, να τυγχάνουν κρυπτογράφησης οι ειδικές κατηγορίες προσωπικών δεδομένων με σκοπό τον περιορισμό των επιπτώσεων μη εξουσιοδοτημένης πρόσβασης[292]. Στο πλαίσιο αυτό, αξίζει να αναφερθεί ότι μέσω της Οδηγίας NIS 2, η οποία σκοπεύει μεταξύ άλλων στην ενίσχυση των μέτρων της κυβερνοασφάλειας καθώς και της κυβερνοανθεκτικότητας εντός της Ε.Ε. θα μπορούσε να υπάρξει μεγαλύτερη κυβερνοπροστασία και εντός του metaverse.

[289] Dwivedi, K. Y. et al. (2022), ό.π., σελ. 8

[290] Pietro, Di R., and Cresci, S. (2021), ό.π., σελ. 285

[291] Αναφορικά με το ζήτημα της προστασίας της ιδιωτικότητας, έχει γίνει πλήρης αναφορά στο αντίστοιχο κεφάλαιο της παρούσας.

[292] Dwivedi, K. Y. et al. (2022), ό.π., σελ. 8

Επιπροσθέτως, κρίνεται απαραίτητη η ύπαρξη πολιτικών προστασίας της ιδιωτικής ζωής, όπως αναφέρθηκε και στο αντίστοιχο κεφάλαιο περί προσωπικών δεδομένων της παρούσας, στις οποίες θα μπορούν να συμπεριλαμβάνονται προβλέψεις προστασίας της κυβερνοασφάλειας καθώς και η διενέργεια διαφόρων σχετικών προγραμμάτων συμμόρφωσης εκ μέρους των δημιουργών του metaverse[293]. Πέραν τούτων, θα πρέπει οι πιο κρίσιμες ρυθμίσεις ασφαλείας να διαμορφώνονται ορθά αλλά αναγκαίο είναι να εκπαιδεύονται και οι χρήστες προκειμένου να αναγνωρίζουν επικίνδυνα περιστατικά ασφαλείας π.χ. αποτροπή επιθέσεων κοινωνικής μηχανικής (social engineering) στο metaverse, οι οποίες συνιστούν το μεγαλύτερο ποσοστό επιθέσεων στον κυβερνοχώρο ιδίως ενόσω διαρκούσε η πανδημία Covid-19[294] καθώς και να εκπαιδεύονται αναφορικά με τα μέτρα που δύνανται να λάβουν με σκοπό την προστασία τόσο της ταυτότητάς τους όσο και των ψηφιακών περιουσιακών τους στοιχείων[295]. Τα εν λόγω μέτρα κυβερνοασφάλειας θα πρέπει να ελέγχονται σε τακτική βάση[296]. Θα μπορούσε, συνεπώς, να δίνεται μεγάλη σημασία στον ίδιο το χρήστη, με την έννοια ότι τούτος θα κατέχει την απόλυτη εξουσία επί των δεδομένων του, αφού προηγουμένως έχει ενημερωθεί κατάλληλα και επαρκώς. Οι δε προγραμματιστές θα πρέπει να δημιουργήσουν τα κατάλληλα πρωτόκολλα κυβερνοασφάλειας προς το σκοπό της προστασίας των βιομετρικών ιδίως δεδομένων[297].

Σε ένα πλαίσιο, επομένως, στο οποίο οι εταιρείες αγωνίζονται με σκοπό να εδραιώσουν τη θέση τους στον ανταγωνισμό δεν θα πρέπει να παραβλέπουν εξ αρχής και εκ των προτέρων την ανάγκη ύπαρξης ενός ασφαλούς metaverse, κάτι το οποίο θα μπορούσε να γίνει μέσω της ασφάλειας ήδη από το σχεδιασμό[298]. Ως εκ τούτου, καθίσταται σαφές ότι η ασφάλεια και ιδιωτικότητα κάθε άλλο παρά προαιρετικές πρέπει να είναι εντός του metaverse, πρέπει δε να υφίστανται καθ' όλη τη διάρκεια και σε όλα τα επίπεδα παροχής υπηρεσιών καθώς και καθ'όλες τις φάσεις ανάπτυξης και συντήρησης των προϊόντων και υπηρεσιών του metaverse. Ιδίως αναφορικά με τη μέριμνα των εταιρειών για ύπαρξη ασφαλείας ήδη από το σχεδιασμό, θα πρέπει η εταιρεία/δημιουργός του metaverse να είναι

---

[293] Ara, T. et al., (2022), 'Exploring the metaverse: What laws will apply?'. Διαθέσιμο σε: https://www.dlapiper.com/en/insights/publications/2022/02/exploring-the-metaverse (Τελευταία πρόσβαση: 16.06.2023)

[294] Pietro, Di R., and Cresci, S. (2021), ό.π., σελ. 284

[295] Madiega, T., Car, P. et aI., (2022), ό.π., σελ. 9

[296] Petrányi, D., Horváth, K. and Domokos, M. (2022) 'Part 3 - Data protection challenges, the importance of cybersecurity, advertising regulation in the metaverse', ό.π.

[297] Buck, L. and McDonell, R. (2022), ό.π., σελ.2

[298] Europol (2022), ό.π., σελ. 13

σε θέση να αυτοματοποιεί, επί παραδείγματι, τους ελέγχους ασφάλειας των δεδομένων καθώς και να ενσωματώσει ήδη από την αρχή της δημιουργίας του περιβάλλοντος την ασφάλεια στις διαδικασίες διαχείρισης των πληροφοριακών συστημάτων της. Στο πλαίσιο αυτό, τόσο τα προϊόντα π.χ. περιεχόμενο και λογισμικό όσο και οι υπηρεσίες είναι αναγκαίο να σχεδιάζονται και να λαμβάνουν χώρα με τρόπο που να διασφαλίζεται ότι πληρούνται οι βασικές έννοιες της κυβερνοασφάλειας ήτοι το λεγόμενο CIA (εμπιστευτικότητα – διαθεσιμότητα – ακεραιότητα). Ωστόσο, είναι κρίσιμο να υπάρξουν προηγμένες τεχνολογίες προστασίας της ασφάλειας π.χ. «*αυτοματοποιημένος, ευέλικτος, κρυπτογραφημένος έλεγχος της πρόσβασης στα δεδομένα με χρήση τεχνητής νοημοσύνης*»[299] προκειμένου να ανταποκρίνονται με κατάλληλο τρόπο στις ιδιαιτερότητες του περιβάλλοντος του metaverse.

Αναφορικά με το ζήτημα της αυτοματοποίησης των διαδικασιών και του αυτοματοποιημένου ελέγχου, αξίζει να σημειωθεί ότι πράγματι σε περιβάλλοντα όπως το metaverse, όπου υφίσταται αναρίθμητη επεξεργασία προσωπικών δεδομένων και οι κίνδυνοι κυβερνοασφάλειας είναι εμφανείς, θα ήταν προτιμότερη η προώθηση της αυτοματοποίησης εκ μέρους των πλατφορμών, υπό την έννοια ότι θα μπορούσε η πλειονότητα του χειρισμού των εργασιών και λειτουργιών να πραγματοποιηθεί μέσω αλγορίθμων τεχνητής νοημοσύνης αντί μέσω ανθρώπων. Ωστόσο, δεν πρέπει να λησμονηθεί ότι ήδη στη σημερινή μορφή του διαδικτύου, έχουν υπάρξει δυσμενείς συνέπειες λόγω της ανάθεσης κοινωνικά ουσιωδών εργασιών σε αλγορίθμους, συνέπειες που σχετίζονται, μεταξύ άλλων, με τις προκαταλήψεις, την αδιαφάνεια κ.λπ[300].

Προς επίλυση του ζητήματος της κλοπής της ταυτότητας του άβαταρ και εν συνεχεία καταχρηστικής χρήσεως τούτης καθώς και με σκοπό την πρόληψη της απάτης μια λύση θα μπορούσε να δοθεί μέσω της πιστοποίησης της ταυτότητας του χρήστη που να βασίζεται στην τεχνολογία blockchain, η οποία λόγω του ότι λειτουργεί με βάση ένα αποκεντρωμένο σύστημα και δεν υπάρχει παρέμβαση κάποιου κεντρικού φορέα, είναι πιο ανθεκτική σε ζητήματα κυβερνοασφάλειας και διασφαλίζει την ιχνηλασιμότητα και διαφάνεια. Προκειμένου το εν λόγω σύστημα να είναι πράγματι ισχυρό και ανθεκτικό θα πρέπει να έχει τη μορφή ενός αποκεντρωμένου δικτύου ταυτοποίησης που να περιέχει σύστημα επαλήθευσης λογαριασμού, το οποίο θα φέρει τις εγγυήσεις διεθνών προτύπων[301]. Μια

[299] Dwivedi, K. Y. et al. (2022), ό.π., σελ. 9
[300] Pietro, Di R., and Cresci, S. (2021), ό.π., σελ. 285
[301] Madiega, T., Car, P. et aI., (2022), ό.π., σελ. 9

εναλλακτική λύση θα ήταν η ύπαρξη μηχανισμών πιστοποίησης της ταυτότητας και αυθεντικοποίησης του χρήστη, οι οποίοι θα είναι γρήγοροι όπως π.χ. η βιομετρική αυθεντικοποίηση[302]. Σημειωτέον ότι είναι απαραίτητο σε κάθε περίπτωση οι πλατφόρμες του metaverse να εφαρμόζουν μια ισχυρή διαδικασία πιστοποίησης (know your customer) με απώτατο σκοπό την αποτροπή υποκλοπής της ταυτότητας ενός χρήστη και εγκαθίδρυσης ενός κλίματος εμπιστοσύνης μεταξύ των χρηστών ενώ παράλληλα και διευκόλυνσης αρμόδιων των αρχών να πραγματοποιήσουν έρευνες περί των διαπραττόμενων αδικημάτων εντός της πλατφόρμας του metaverse[303].

Περαιτέρω, καθώς μέσω των συσκευών π.χ. ακουστικά εικονικής πραγματικότητας, πραγματοποιούνται βασικές λειτουργίες στο metaverse, θα πρέπει και οι καθαυτές συσκευές να είναι ασφαλείς και να ενημερώνονται διαρκώς για νέες επιδιορθώσεις σε ζητήματα ασφαλείας[304]. Εν προκειμένω το νέο ευρωπαϊκό καθεστώς μπορεί να ενισχύσει την προστασία του καταναλωτή χρήστη αναφορικά και με τις εν λόγω συσκευές. Ειδικότερα, οι εν λόγω συσκευές π.χ. VR, AR, μπορεί ως καταναλωτικά προϊόντα να μην εμπίπτουν στο πεδίο εφαρμογής της Οδηγίας NIS 2, η οποία δεν καλύπτει απαιτήσεις κυβερνοασφάλειας για τα εν λόγω προϊόντα, αλλά εμπίπτουν στο πεδίο εφαρμογής του νέου Κανονισμού περί της γενικής ασφάλειας των προϊόντων[305], ο οποίος αναφέρεται, μεταξύ άλλων, στην ύπαρξη κατάλληλων χαρακτηριστικών κυβερνοασφάλειας με σκοπό την προστασία των προϊόντων[306].

Τέλος, πρέπει να ενισχυθεί και η ασφάλεια του δικτύου, ήτοι να υφίσταται κρυπτογράφηση στη σύνδεση δικτύου με τη χρήση ασφαλούς και αποτελεσματικού αλγορίθμου κρυπτογράφησης καθώς και να υφίσταται η κατάλληλη προετοιμασία, σε περιπτώσεις όπου επί παραδείγματι ανακύψει μια επίθεση DDos, ήτοι να υπάρχει εξαρχής ένα «*σχέδιο επιχειρησιακής συνέχειας και αποκατάστασης από καταστροφές*»[307] ιδίως σε κρίσιμα και πολύ σημαντικά συστήματα. Επίσης, προκειμένου να αντιμετωπιστούν

---

[302] Cheng S., Zhang Y., Li X., et al., (2022), ό.π., σελ.2
[303] Europol (2022), ό.π., σελ.14
[304] Dwivedi, K. Y. et al. (2022), ό.π., σελ. 8
[305] *Κανονισμός (ΕΕ) 2023/988 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 10ης Μαΐου 2023 για τη γενική ασφάλεια των προϊόντων, την τροποποίηση του κανονισμού (ΕΕ) αριθ. 1025/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και της οδηγίας (ΕΕ) 2020/1828 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, και την κατάργηση της οδηγίας 2001/95/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και της οδηγίας 87/357/ΕΟΚ του Συμβουλίου.* Διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32023R0988 (Τελευταία πρόσβαση: 16.06.2023)
[306] Madiega, T., Car, P. et al., (2022), ό.π., σελ. 8
[307] Dwivedi, K. Y. et al. (2022), ό.π., σελ. 8

ζητήματα κυβερνοασφάλειας στο πλαίσιο της διαλειτουργικότητας και να μπορούν οι χρήστες να μετακινούνται απρόσκοπτα από τον έναν εικονικό χώρο σε άλλον, θα πρέπει να υπάρξουν ισχυρά πρωτόκολλα, τα οποία θα δύνανται να περιορίσουν τον κίνδυνο μεταφοράς επιβλαβών στοιχείων μεταξύ των επιμέρους πλατφορμών[308].

6.2. Metaverse και ασφάλεια των χρηστών

Πέραν των ως άνω ζητημάτων που άπτονται του πεδίου της κυβερνοασφάλειας, ενδέχεται να υπάρξουν και ζητήματα ασφαλείας από την άποψη των αδικημάτων του ποινικού δικαίου, εις βάρος ενός άβαταρ – χρήστη. Ειδικότερα, οι αλληλεπιδράσεις μεταξύ των άβαταρ εντός του περιβάλλοντος του metaverse, δύναται να δημιουργήσουν καταστάσεις, οι οποίες συνιστούν αδικήματα του πραγματικού κόσμου π.χ. σωματική ή προφορική επίθεση εις βάρος ενός άβαταρ σε συνέχεια μιας ενέργειας άλλου άβαταρ, σεξουαλική παρενόχληση ενός άβαταρ, όπως μάλιστα συνέβη και στην πραγματικότητα τελευταία σε μια Βρετανίδα χρήστη[309], ο διαδικτυακός εκφοβισμός[310], εν γένει ζητήματα κακής συμπεριφοράς, ανεπιθύμητης αλληλογραφίας[311], μαζικής παρακολούθησης[312] κ.λπ. Υποστηρίζεται δε ότι οι πιο κοινές περιπτώσεις βλαβών εντός του metaverse θα είναι ψυχολογικής και συναισθηματικής μορφής[313].

Μεταξύ, συνεπώς, των σοβαρών αδικημάτων, τα οποία δύνανται να λάβουν χώρα εντός του metaverse, είναι το αδίκημα του βιασμού καθώς και περιστατικά σεξουαλικής παρενόχλησης γυναικών. Ειδικότερα, ήδη έχουν εμφανιστεί στην πλατφόρμα metaverse κοινωνικής δικτύωσης εικονικής πραγματικότητας της Meta περιστατικά σεξουαλικής παρενόχλησης εις βάρος γυναικών[314]. Από την άλλη, το 2007, υπήρξε περιστατικό στην πλατφόρμα Second Life όπου ένα άβαταρ βίασε ένα άλλο, δημιουργώντας αυτομάτως το ερώτημα του πώς δύναται σε τέτοιες περιπτώσεις να εφαρμοστεί ορθά η ισχύουσα νομοθεσία με δεδομένο ότι, επί παραδείγματι, το αδίκημα του βιασμού απαιτεί σωματική επαφή ενώ το άβαταρ έχει εικονική υπόσταση. Παρόλα αυτά, δεν πρέπει να λησμονείται το γεγονός ότι το metaverse παρέχει μια εμβυθιστική εμπειρία με αποτέλεσμα να είναι δύσκολη

[308] Madiega, T., Car, P. et aI., (2022), ό.π., σελ. 8
[309] Κόκιου, Β. (2022), ό.π.
[310] Pietro, Di R., and Cresci, S. (2021), ό.π., σελ. 285
[311] Fernandez, C.B and Hui, P. (2022), ό.π., σελ.274
[312] Κουσουνή-Πανταζοπούλου, Α. (2023), ό.π. σελ. 382
[313] Cheong, B.C. (2022), ό.π., σελ. 477
[314] Madiega, T., Car, P. et aI., (2022), ό.π., σελ. 6

η οριοθέτηση του εικονικού με του πραγματικού κόσμου και οι εμπειρίες που βιώνει ένας χρήστης μέσω του άβαταρ του μοιάζουν πραγματικές και μπορούν να επιδράσουν σε αυτόν, όπως μια εμπειρία του φυσικού κόσμου[315].

Συνεπώς, η εμφάνιση τέτοιου είδους αδικημάτων καθίσταται εντονότερη από το γεγονός ότι το metaverse συνιστά μια τεχνολογία εμβύθισης που παρέχει μια «*σουρεαλιστική εμπειρία*», δίνοντας ταυτόχρονα την ευκαιρία σε χρήστες να παρουσιάζουν κακοποιητικές συμπεριφορές εις βάρος άλλων χρηστών[316]. Παρά το γεγονός δηλαδή ότι οι εν λόγω καταστάσεις λαμβάνουν χώρα σε ένα εικονικό περιβάλλον, για τον εμπλεκόμενο χρήστη νοείται ως μια πραγματική και επιβλαβής εμπειρία[317]. Επίσης, πρόβλημα θα μπορούσε να δημιουργηθεί στην περίπτωση που αποσταλεί ανεπιθύμητο περιεχόμενο μέσω της τεχνολογίας blockhain ή των NFTs, το οποίο από τη στιγμή που υπάρχει σε μια αλυσίδα μπλοκ δεν υφίσταται τρόπος αφαίρεσης τούτου με αποτέλεσμα οιαδήποτε παρενόχληση λαμβάνει χώρα με αυτούς τους τρόπους να εμφανίζεται για αόριστο χρονικό διάστημα στην εν λόγω αλυσίδα προκαλώντας αντιστοίχως δυσμενείς συνέπειες στους χρήστες, οι οποίοι δεν θα δύνανται πρακτικά να απεμπλακούν από το εν λόγω περιστατικό παρενόχλησης[318].

Περαιτέρω, ανάλογου βαθμού ανησυχία δημιουργούν και κίνδυνοι που προέρχονται από άλλες μορφές επικοινωνίας μεταξύ των χρηστών, όπως είναι για παράδειγμα η ανταλλαγή μηνυμάτων σεξουαλικού περιεχομένου με τη χρήση κυρίως κινητού τηλεφώνου (sexting)[319], το οποίο θα μπορούσε να πραγματοποιηθεί και μέσω του metaverse. Το πρόβλημα εν προκειμένω ανακύπτει στην περίπτωση που παραβιαστεί το απόρρητο των εν λόγω επικοινωνιών ιδίως από την άποψη του ποινικού δικαίου, δημιουργώντας ζητήματα εκδικητικής πορνογραφίας[320], τα οποία ήδη λαμβάνουν χώρα στο Web 2.0. και τα οποία θα γινόντουσαν πιο έντονα σε καθηλωτικά περιβάλλοντα, όπως το metaverse. Επίσης, μεταξύ των αδικημάτων, τα οποία δύνανται να λάβουν χώρα εντός του metaverse εξαιτίας παράνομων συμπεριφορών των άβαταρ είναι η συκοφαντική δυσφήμιση και η διακίνηση ναρκωτικών[321].

---

[315] Europol (2022), ό.π., σελ. 17
[316] Bale, A.S. et al. (2022), ό.π., σελ.8
[317] Madiega, T., Car, P. et aI., (2022), ό.π., σελ. 6
[318] Europol (2022), ό.π., σελ. 17
[319] Pietro, Di R., and Cresci, S. (2021), ό.π., σελ. 285
[320] Το αδίκημα της εκδικητικής πορνογραφίας (revenge porn) προβλέπεται πλέον και τιμωρείται και υπό το πρίσμα του ελληνικού ποινικού δικαίου, ήτοι με βάση το άρθρο 346 του Ποινικού Κώδικα.
[321] Cheong, B.C. (2022), ό.π., σελ. 488

Πράγματι, επομένως, υφίσταται το πεδίο εντός του οποίου θα μπορούσε να εκτυλιχθεί μια σειρά παράνομων ενεργειών και δυσμενών συμπεριφορών εντός του metaverse, τα οποία λόγω της φύσης του metaverse είναι καταρχήν δύσκολο να αποτραπούν και να ελεγχθούν. Εγκλήματα, όπως ο εκβιασμός και εκφοβισμός θα μπορούσαν να φέρουν τους χρήστες του metaverse αντιμέτωπους με επικίνδυνα περιστατικά ενώ μέσω των κυβερνοεπιθέσεων βιομετρικά δεδομένα των χρηστών θα μπορούσαν να πωληθούν στο dark web, κάτι το οποίο θα είχε εξαιρετικά δυσμενείς επιπτώσεις για την ιδιωτικότητα των χρηστών εντός του metaverse[322].

Άλλωστε, μέσω των τεχνολογιών επαυξημένης και εικονικής πραγματικότητας δημιουργείται, επίσης, το πρόσφορο έδαφος για λεκτική παρενόχληση, ρητορική μίσους, δημιουργία πορνογραφικού περιεχομένου, παραπληροφόρηση, δυσφημιστικό περιεχόμενο, εξάπλωση εξτρεμιστικών ιδεολογιών[323]. Αναφορικά ιδίως με το ζήτημα της παραπληροφόρησης, αξίζει να αναφερθεί ότι, ήδη η σημερινή μορφή του διαδικτύου (Web2.0) παρέχει τη δυνατότητα με ακρίβεια στόχευσης ορισμένων κοινωνικών ομάδων προκειμένου να ασκηθεί επίδραση στη συμπεριφορά τους, κάτι το οποίο θα ενταθεί στο metaverse λόγω του ότι η άσκηση επιρροής στη συμπεριφορά του χρήστη θα διευκολύνεται στο metaverse λόγω της συλλογής πολλών δεδομένων από τις τεχνολογικές συσκευές σύνδεσης στο metaverse, από τους χρήστες π.χ. για εμπορικούς ή πολιτικούς σκοπούς. Με την υιοθέτηση δε της τεχνολογίας Web3.0, η παραπληροφόρηση θα είναι αδύνατο να εξαφανιστεί με δεδομένο ότι θα μπορεί η διάδοση της να γίνει πιο αποκεντρωμένη λόγω της νέας ως άνω τεχνολογίας. Στο πλαίσιο αυτό, αξίζει να αναφερθεί ότι η δομή του metaverse επιτρέπει τη δημιουργία μεγάλης ποσότητας ψηφιακών ιχνών που σχετίζεται με τη μεγάλη ποσότητα δεδομένων και έτσι μπορεί να υπάρξει δυνατότητα ταυτοποίησης του ατόμου καθώς και εν δυνάμει πρόβλεψη της συμπεριφοράς του και κατά συνέπεια προσαρμογή του περιεχομένου σύμφωνα με τις εν λόγω πληροφορίες, τη χειραγώγηση του ατόμου καθώς και τον εντοπισμό του[324].

Επιπροσθέτως, μέσω του metaverse θα μπορούσαν να εμφανιστούν με εντονότερο τρόπο εγκλήματα σχετικά με την τρομοκρατία και τη σύσταση τρομοκρατικών οργανώσεων καθώς και την προπαγάνδα. Είναι άλλωστε γνωστό ότι οι τρομοκράτες πάντοτε

[322] Buck, L. and McDonell, R. (2022), ό.π., σελ. 2
[323] Madiega, T., Car, P. et aI., (2022), ό.π., σελ. 6
[324] Europol (2022), ό.π., σελ. 20

ενδιαφέρονται για την ανίχνευση και εκμετάλλευση νέων τεχνολογικών επιλογών με σκοπό να πετύχουν τα συμφέροντά τους. Σε περιβάλλοντα καθηλωτικής εμπειρίας, όπως αυτή που παρέχει το metaverse, θα μπορούν οι τρομοκράτες να επιλέγουν τα ευάλωτα άτομα - στόχους τους και να ρυθμίζουν τα μηνύματά τους προς αυτούς προκειμένου να ικανοποιούν τα συμφέροντά τους. Σε άλλες περιπτώσεις, θα μπορούσε να δημιουργηθεί εντός του metaverse ένας παράλληλος κόσμος, ο οποίος να καταλύει και να υπονομεύει την έννοια του κράτους δικαίου, να λειτουργεί, δηλαδή, με κανόνες που βρίσκονται σε σαφή αντίθεση με τις βασικές θεμελιώδεις αρχές και αξίες του φυσικού κόσμου καθώς και να προωθεί τρομοκρατικές δραστηριότητες με εκτάσεις που μπορούσαν να επηρεάσουν και το φυσικό κόσμο[325].

Ένα άλλο πρόβλημα, το οποίο θα μπορούσε να υπάρξει στο metaverse αφορά στις οικονομικές ζημίες λόγω εγκλημάτων, όπως η νομιμοποίηση εσόδων από παράνομες δραστηριότητες (το γνωστό «ξέπλυμα χρήματος») και οι απάτες[326]. Παρά το γεγονός ότι μέσω των NFTs, μπορεί να αποδειχθεί η ιδιοκτησία των ψηφιακών περιουσιακών στοιχείων, το πρόβλημα της παράνομης νομιμοποίησης εσόδων και εντός του metaverse δεν μπορεί να λησμονηθεί καθώς ήδη τα κρυπτονομίσματα συνιστούν ένα μέσο παράνομης νομιμοποίησης εσόδων. Ειδικότερα, είναι δύσκολο για τις αρχές επιβολής του νόμου να παρακολουθούν τις διασυνοριακές μεταφορές χρημάτων εντός του metaverse, στο οποίο προκειμένου να πωληθούν εικονικά αγαθά θα απαιτείται η μεταφορά εικονικών χρημάτων, η οποία ενίοτε θα είναι παράνομη. Στο πλαίσιο αυτό, η ανωνυμία που υφίσταται στο πεδίο των κρυπτονομισμάτων καθιστά την κατάσταση ακόμη πιο δυσχερή για τις αρχές, οι οποίες θα έρχονται αντιμέτωπες με τεράστιες προκλήσεις στην ανίχνευση των δραστών. Τα δε NFTs είναι ένα πρόσφορο μέσο για τα αδικήματα της απάτης και της υπεξαίρεσης καθώς ναι μεν δύναται να αποδείξουν την ιδιοκτησία, η επαλήθευση, ωστόσο, τούτης είναι πρακτικά ανέφικτη λόγω του μεγάλου αριθμού των προσφερόμενων NFTs και ως εκ τούτου μπορεί να υπάρξει μια σειρά παράνομων NFTs[327].

Αξίζει να σημειωθεί ότι το phising, πέραν από ζητήματα κυβερνοασφάλειας, θα μπορούσε να κυριαρχήσει ως παράνομη μέθοδος εντός του metaverse καθώς οι δράστες μέσω του phising θα μπορούσαν να υποδυθούν τόσο εμπορικά σήματα όσο και άλλα άτομα με σκοπό να πείσουν τα θύματά τους ότι πράγματι π.χ. το ψεύτικο εικονικό κατάστημα εντός

[325] Europol (2022), ό.π., σελ. 19
[326] Europol (2022), ό.π., σελ. 15
[327] Europol (2022), ό.π., σελ. 16

του metaverse είναι το αληθινό ή ότι πρόκειται πράγματι για το άτομο το οποίο υποδύεται ο δράστης και άρα να οδηγήσουν το χρήστη σε μια συγκεκριμένη συμπεριφορά με σκοπό, μεταξύ άλλων, την απόσπαση προσωπικών πληροφοριών π.χ. στοιχείων τραπεζικού λογαριασμού[328]. Ενδεικτικά, αξίζει να αναφερθεί η περίπτωση του Roblox, το οποίο συνιστά ένα εκ των εμπορικών σημάτων, που τυγχάνουν σε μεγάλο βαθμό απομίμησης σε απόπειρες ψαρέματος – το λεγόμενο phising εμπορικών σημάτων-, κατάσταση, η οποία εντείνει τις ανησυχίες σε επίπεδο ασφαλείας καθώς η εν λόγω πλατφόρμα χρησιμοποιείται σε μεγάλο βαθμό και από παιδιά, ηλικίας κάτω των 16 ετών[329].

Επιπλέον, πέρα από τις ως άνω οικονομικές ζημίες οι κυβερνοεπιθέσεις κατά των ίδιων των συστημάτων που συνδέουν το χρήστη στο metaverse μπορούν να προκαλέσουν και πραγματική βλάβη του χρήστη στο φυσικό περιβάλλον, ήτοι να προκληθεί σωματική βλάβη στο χρήστη – θύμα, εάν παραβιαστεί, «χακαριστεί», λόγου χάρη ένα σύστημα VR και να μετακινηθεί με αυτόν τον τρόπο ένας χρήστης στον πραγματικό κόσμο σε μια τοποθεσία χωρίς να το καταλάβει π.χ. να πέσει από μια σκάλα και έτσι να τραυματιστεί σοβαρά ή ακόμα χειρότερα εάν παραβιαστεί μια συσκευή τεχνολογίας AR ένας χρήστης θα μπορούσε να μετατραπεί σε θύμα σοβαρών εγκλημάτων όπως π.χ. ληστεία[330] και βαριά σωματική βλάβη.

Σημειωτέον ότι τα προβλήματα ασφαλείας εντός του metaverse γίνονται ακόμη εντονότερα, στην περίπτωση των ανηλίκων χρηστών, οι οποίοι μπορεί να αντιμετωπίσουν ζητήματα βίας, παρενόχλησης καθώς και πορνογραφικού περιεχομένου εντός του metaverse[331]. Ήδη, η παρενόχληση μέσω του διαδικτύου εις βάρος των ανηλίκων συνιστά καίριο ζήτημα με δεδομένο ότι βάσει σχετικής διεθνούς έρευνας το 2020 το 58% των ανηλίκων κοριτσιών έχουν βιώσει διαδικτυακή παρενόχληση[332]. Επί του παρόντος, δεν υφίσταται ηλικιακή διαβάθμιση των εμπειριών που μπορεί να βιώσει ένας χρήστης εντός του metaverse, με αποτέλεσμα τα παιδιά να μπορούν να εκτεθούν σε μια σειρά επικίνδυνων εμπειριών όπως π.χ. ενήλικοι δράστες, οι οποίοι προβαίνουν σε κακοποιητικές ενέργειες εις βάρος των ανηλίκων μέσω των διαφόρων ευκαιριών π.χ. παιχνίδια εντός του metaverse και μάλιστα λόγω της φύσης του metaverse θα είναι αρκετά δύσκολο για έναν ανήλικο να

[328] Europol (2022), ό.π., σελ. 15
[329] Europol (2022), ό.π., σελ. 13
[330] Dwivedi, K. Y. et al. (2022), ό.π., σελ. 10
[331] Dwivedi, K. Y. et al. (2022), ό.π., σελ. 8
[332] Europol (2022), ό.π., σελ. 16

διακρίνει τους ενήλικες από άλλους ανηλίκους και να γνωρίζει με ποιον πράγματι επικοινωνεί κάθε φορά.

Επομένως, το φαινόμενο «grooming» ανηλίκων καθώς και κάθε σχετική μορφή εκμετάλλευσης των ανηλίκων θα μπορούσε να λάβει τεράστιες και επικίνδυνες διαστάσεις εντός του metaverse καθώς τα υπάρχοντα εμπόδια για τους δράστες π.χ. πρώτα να έρθουν σε επικοινωνία με ένα παιδί μέσω λόγου χάρη ενός chatroom και έπειτα να το πείσουν να τους δώσει τα προσωπικά του στοιχεία δεν υφίστανται στο metaverse, το οποίο τουναντίον με τις εξελίξεις στην τεχνολογία αφής θα μπορούσε να γίνει ακόμα πιο επικίνδυνο για τα παιδιά, τα οποία θα μπορούσαν να υπάρξουν θύματα πραγματικής σεξουαλικής κακοποίησης εντός της κατοικίας τους μέσω των απτικών συσκευών που θα χρησιμοποιεί δυνητικά ένα παιδί και δίχως ο δράστης να έχει μετακινηθεί καν από τη δική του κατοικία[333]. Άλλος ένας ακόμη κίνδυνος που αφορά ιδίως στους ανηλίκους θα ήταν ο κίνδυνος της παράνομης παιδικής εργασίας καθώς σε πολλές περιπτώσεις τα παιδιά θα μπορούσαν να κληθούν να εργαστούν για τη δημιουργία εμπειριών για πλατφόρμες που σκοπό θα έχουν την απόκτηση χρημάτων, τα οποία δεν θα διανέμονται με ορθό και ομοιόμορφο τρόπο για όλους τους συνεισφέροντες στην εκάστοτε σχετική εργασία[334].

Προκειμένου να αντιμετωπιστούν οι ως άνω κίνδυνοι ασφαλείας και να μπορεί ένας χρήστης να «κυκλοφορεί» και να χρησιμοποιεί το metaverse δίχως να βρίσκεται συνεχώς αντιμέτωπος με τις εν λόγω προκλήσεις θα πρέπει πέραν των μέτρων κυβερνοασφάλειας και προστασίας των προσωπικών δεδομένων που αναφέρθηκαν ανωτέρω να ληφθούν υπόψιν και άλλοι παράγοντες και μέτρα. Τούτο διότι, αν δεν υπάρξει πρόνοια για λήψη μέτρων με σκοπό τον περιορισμό των εγκλημάτων εντός του metaverse, τότε το τελευταίο θα μπορούσε να αναδειχθεί ως ένας ιδιαίτερα επικίνδυνος κόσμος, ο οποίος μπορεί να επηρεάσει πολύ αρνητικά την ψυχική υγεία των ατόμων - χρηστών[335].

Καταρχάς είναι σημαντικό να ξεκαθαριστεί το τι θεωρείται εγκληματική συμπεριφορά εντός του metaverse (π.χ. η έννοια των σωματικών πράξεων στην περίπτωση της σεξουαλικής κακοποίησης θα πρέπει να ερμηνευτεί εκ νέου υπό τους όρους του metaverse) και να αντιμετωπίζεται πάντοτε η εν λόγω συμπεριφορά από τις κατάλληλες νομοθετικές προβλέψεις, οι οποίες θα δίνουν τα κατάλληλα μέσα για την ποινική δίωξη των

[333] Europol (2022), ό.π., σελ. 18
[334] Europol (2022), ό.π., σελ. 18-19
[335] Bale, A.S. et al. (2022), ό.π., σελ. 8

εν λόγω αδικημάτων. Είναι πολύ σημαντικό να δημιουργηθούν οι κατάλληλες ρυθμίσεις, εφόσον δεν υφίστανται ήδη, για τα αδικήματα εντός του metaverse καθώς και η λήψη κατάλληλων μέτρων και κατάλληλων μεθόδων ανίχνευσης των εγκλημάτων και απομάκρυνσης των δραστών. Συνεπώς, θα πρέπει να διερευνηθεί εκ νέου υπό το πρίσμα του metaverse το ποια αποκλίνουσα συμπεριφορά εντός του metaverse θα θεωρείται παράνομη ενώ καθίσταται αναγκαίος ο καθορισμός των απαραίτητων νομικών και τεχνικών μέσων[336] προς όφελος των θυμάτων. Η τεχνολογία blockchain εν προκειμένω θα μπορούσε να θεωρηθεί ως μέσο χορήγησης των κατάλληλων πληροφοριών σχετικά με κάποιον δράστη[337]. Οι δε αρχές επιβολής του νόμου πρέπει να είναι πάντοτε ενήμερες σχετικά με τις εξελίξεις στον τομέα των NFTs προκειμένου να είναι σε θέση να προλαμβάνουν και να αντιμετωπίζουν επαρκώς τυχόν εγκλήματα, τα οποία πραγματοποιούνται με τη χρήση NFTs[338] δεδομένου ότι η προστασία κατά της νομιμοποίησης εσόδων από παράνομες δραστηριότητες θα καθίσταται εξίσου σημαντική, όπως και στον πραγματικό κόσμο[339].

Σε κάθε περίπτωση, θα πρέπει να υπάρχει ορθή διακυβέρνηση του εν λόγω εικονικού κόσμου με την κατάλληλη ρύθμιση της συμπεριφοράς εκάστοτε χρήστη, ο οποίος θα υποχρεούται να συμμορφώνεται με τις πολιτικές της εκάστοτε πλατφόρμας του metaverse προκειμένου να αποφεύγονται παράνομες συμπεριφορές και να γνωρίζουν εκ των προτέρων οι χρήστες ότι δεν μπορούν να χρησιμοποιούν το metaverse ως μέσο διενέργειας παραβατικών συμπεριφορών π.χ. χρήση του metaverse με σκοπό τη σεξουαλική παρενόχληση άλλου άβαταρ. Αναγκαίος στο πλαίσιο αυτό είναι και ο καθορισμός των κυρώσεων των εν λόγω συμπεριφορών, ζήτημα το οποίο θέτει μια σειρά από πρακτικές προκλήσεις[340].

Επιπλέον, θα πρέπει να εξασφαλίζεται με κάθε δυνατό μέσο εκ μέρους των πλατφορμών του metaverse η δημιουργία ενός ασφαλούς περιβάλλοντος για τους ανηλίκους, παρέχοντας τις κατάλληλες εγγυήσεις έναντι κακοποιητικών εμπειριών, ελέγχοντας τυχόν συμπεριφορές που αντιβαίνουν στους όρους χρήσης της εκάστοτε πλατφόρμας και εντοπίζοντας έναν αποτελεσματικό τρόπο προστασίας των ανηλίκων από την έκθεση τους σε ακατάλληλο για την ηλικία τους περιεχόμενο[341]. Ιδιαίτερα σημαντική

[336] Europol (2022), ό.π., σελ. 17-18
[337] Europol (2022), ό.π., σελ.17
[338] Europol (2022), ό.π., σελ.16
[339] Europol (2022), ό.π., σελ.15
[340] Fernandez, C.B and Hui, P. (2022), ό.π., σελ.272
[341] Europol (2022), ό.π., σελ.16

είναι η θέση σε εφαρμογή εκ μέρους των φορέων εκμετάλλευσης του metaverse αυστηρών μηχανισμών ελέγχων επιβλαβούς περιεχομένου, το οποίο θα φιλτράρεται και διαγράφεται, ούτως ώστε να διασφαλιστεί η εμπόδιση τέτοιου είδους φαινομένων[342].

Τέλος, αναφορικά με την πιθανή σύνδεση μεταξύ του dark web και του metaverse θα πρέπει και στην εν λόγω περίπτωση να πραγματοποιηθούν οι κατάλληλες ενέργειες π.χ. με τη δημιουργία ενός κατάλληλου ποινικού συστήματος, το οποίο θα προλαμβάνει και θα τείνει στον περιορισμό τέτοιου είδους παράνομων δραστηριοτήτων[343]. Όλα τα εν λόγω μέτρα θα μπορέσουν να ενισχύσουν και την αστυνόμευση εντός του metaverse, η οποία φαίνεται να είναι δυσχερής λόγω κυρίως της μη ύπαρξης των σχετικών διαθέσιμων πόρων εξαιτίας της συνεχούς αύξησης των νέων πλατφορμών αλλά και της δυσχέρειας ελέγχου όχι τόσο του περιεχομένου αλλά της συμπεριφοράς του δράστη, η οποία δεν είναι πάντοτε (ευκόλως) ανιχνεύσιμη εντός του metaverse[344].

[342] Συμβουλευτική Επιτροπή Βιομηχανικών Μεταλλαγών (2023), *Πρωτοβουλία για τους εικονικούς κόσμους, όπως το μετασύμπαν (metaverse).* Διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=PI_EESC:EESC-2023-00888-AS (Τελευταία πρόσβαση: 16.06.2023)

[343] Madiega, T., Car, P. et aI., (2022), ό.π., σελ. 8

[344] Κουσουνή-Πανταζοπούλου, Α. (2023), ό.π. σελ. 385

7. ΣΥΜΠΕΡΑΣΜΑ

Συνοψίζοντας, μπορεί ένα πλήρως λειτουργικό metaverse να απέχει ακόμα αρκετά έτη[345] καθώς κατά μία άποψη απαιτούνται τουλάχιστον έξι με οκτώ χρόνια μέχρι να καταστεί διαθέσιμο «*το πλήρες δυναμικό του metaverse*»[346], αλλά ήδη επί του παρόντος τα οφέλη φαίνονται ιδιαιτέρως σημαντικά καθώς οι ευκαιρίες που παρέχει και θα παρέχει μελλοντικά το metaverse είναι πολύ καθοριστικές για την καθημερινότητα των χρηστών. Βάσει ερευνών έχει αποδειχθεί ότι το metaverse «*θα επηρεάσει σημαντικά τον τρόπο με τον οποίο συμπεριφερόμαστε και αλληλεπιδρούμε, με το 25% από εμάς να ξοδεύει τουλάχιστον 1 ώρα την ημέρα στο metaverse μέχρι το 2026*»[347]. Αναμένεται δε ότι μέχρι το 2040 το metaverse θα αποτελεί σε παγκόσμιο επίπεδο μια πλήρως εμβυθιστική και πραγματικά λειτουργική πτυχή της καθημερινότητας για μισό δισεκατομμύριο ή περισσότερους ανθρώπους[348]. Προοδευτικά, επομένως, εμφανίζεται μια δεύτερη ζωή, μια ψηφιακή ζωή σε μια κοινωνία όπου με τον καλύτερο δυνατό τρόπο θα συνδυάζονται οι πραγματικοί και οι ψηφιακοί άνθρωποι έχοντας και ως χρήσιμο εργαλείο την τεχνητή νοημοσύνη[349].

Το γεγονός δε ότι, επί του παρόντος, δεν υφίσταται ξεχωριστό νομοθέτημα που να ρυθμίζει αποκλειστικά και μόνο τις σχέσεις και τις συνθήκες του metaverse, δεν φαίνεται κατά την παρούσα χρονική περίοδο να προβληματίζει τους νομοθέτες. Ωστόσο, με δεδομένο ότι ήδη διαφαίνονται σημαντικές προκλήσεις από τη λειτουργία του metaverse, οι οποίες κατά πάσα πιθανότητα θα αυξηθούν, ίσως μελλοντικά δημιουργήσει κάποια κενά δικαίου ή αδυναμία εφαρμογής των παρόντων νομοθετημάτων, κάτι το οποίο δεν μπορεί με βεβαιότητα να προβλεφθεί λόγω της φύσης του metaverse, ως μιας τεχνολογίας, η οποία ήδη έχει εξελιχθεί σημαντικά σε σύγκριση με την πρώτη φορά που αναφέρθηκε η εν λόγω έννοια το 1992 και σε συνέχεια της δημιουργίας των πρώτων περιβαλλόντων metaverse.

Η ίδια η φύση του metaverse έχει δημιουργήσει έντονες συζητήσεις ιδίως ως προς τα προβλήματα που έχουν ξεκινήσει να ανακύπτουν και θα συνεχίζουν να υφίστανται, αν δεν ληφθούν τα κατάλληλα μέτρα, στους τομείς που αναλύθηκαν στην παρούσα. Καταρχάς, στο επίπεδο των προσωπικών δεδομένων, φαίνεται ότι η επεξεργασία βιομετρικών δεδομένων θα κυριαρχήσει στο πεδίο του metaverse και ως εκ τούτου ήδη ευθύς εξαρχής πρέπει

[345] Angeles, J. (2022), ό.π., σελ. 295
[346] Maciejewski, M. (2023), ό.π., σελ. 145
[347] Plechatá, A., Makransky, G. and Böhm, R. (2022), ό.π., σελ. 3
[348] Maciejewski, M. (2023), ό.π., σελ. 21
[349] Cheng S., Zhang Y., Li X., et al., (2022), ό.π., σελ.2

καταρχήν οι πλατφόρμες - πάροχοι του metaverse να είναι προετοιμασμένες και να έχουν λάβει τα απαραίτητα μέτρα και πολιτικές προκειμένου να προστατεύεται στο έπακρο η ιδιωτικότητα και τα προσωπικά δεδομένα του υποκειμένου των δεδομένων, εν προκειμένω του χρήστη του metaverse.

Στο ίδιο πλαίσιο τίθενται διάφορα ερωτήματα αναφορικά με το πώς θα αντιμετωπιστούν ζητήματα ευθύνης εντός του metaverse με βασικό ερώτημα του ποιος ευθύνεται για τα αδικήματα που προκαλεί ένα άβαταρ στο metaverse. Η απάντηση, εν προκειμένω, δεν είναι απλή με δεδομένη την πολυπλοκότητα που υπάρχει στο metaverse, λαμβάνοντας υπόψιν ότι από τη μία σε ένα βαθμό ο χρήστης μπορεί να καλυφθεί από το πέπλο ανωνυμίας, από την άλλη ο προγραμματιστής αν θεωρηθεί υπεύθυνος θα μπορεί να περιοριστεί μελλοντικά η καινοτομία και τέλος το ίδιο το άβαταρ για να θεωρηθεί υπεύθυνο θα πρέπει να αποκτήσει με κάποιο τρόπο νομική προσωπικότητα. Βέβαια, δεν υφίστανται μόνο ζητήματα αστικής ευθύνης εντός του metaverse εκ μέρους των άβαταρ αλλά δύναται να υπάρξει και παράνομο περιεχόμενο και ως εκ τούτου τίθεται το ζήτημα κατά πόσον ευθύνεται η πλατφόρμα για το εν λόγω περιεχόμενο. Η DSA έρχεται στο σημείο αυτό να συνδράμει ουσιωδώς με το να δίνει καταρχήν στην εκάστοτε πλατφόρμα τη δυνατότητα να απαλλαγεί υπό προϋποθέσεις από την ευθύνη της.

Σημειωτέον ότι και εντός του metaverse δύνανται να υπάρξουν ζητήματα ρύθμισης της αγοράς καθώς και προστασίας του ελεύθερου ανταγωνισμού με δεδομένο ότι θα μπορούσαν να εφαρμοστούν οι υπάρχουσες αντιμονοπωλιακές νομοθετικές προβλέψεις, ούτως ώστε να μην παρατηρηθούν καταχρηστικές συμπεριφορές και με σκοπό να περιοριστούν ήδη εξαρχής οι αθέμιτες συμπεριφορές που δύνανται, μεταξύ άλλων, να οδηγήσουν σε επικράτηση μίας ισχυρής πλατφόρμας και μόνο, η οποία να έχει «εξαφανίσει» από την αγορά τις μικρότερες και λιγότερο ισχυρές πλατφόρμες. Σημαντικός στο σημείο αυτό είναι ο ρόλος των αρχών ανταγωνισμού, οι οποίες πρέπει να είναι σε ετοιμότητα για να προλάβουν τέτοια περιστατικά π.χ. κατάχρηση δεσπόζουσας θέσης εντός του metaverse.

Σαφώς δε, εντός του metaverse δεν υφίστανται περιθώρια μη λήψης υπόψιν της κυβερνοασφάλειας αλλά και της μέριμνας για τυχόν διάπραξη ποινικών αδικημάτων, τα οποία δύνανται να έχουν επιπτώσεις και στον πραγματικό κόσμο. Πιο συγκεκριμένα, και εντός του metaverse θα ανακύψουν πιθανότατα ουσιώδη ζητήματα ασφαλείας θέτοντας εξ αρχής ως αναγκαία απαίτηση τον ορθό σχεδιασμό και λήψη κατάλληλων μέτρων

κυβερνοασφάλειας και τεχνικών λύσεων[350]. Από την άλλη σαφώς θα πρέπει να υπάρξει νομοθετική μέριμνα σχετικά με τις κυρώσεις επί των ποινικών αδικημάτων που προκαλούνται εις βάρος άλλων χρηστών εντός του metaverse.

Τέλος, όλες οι πτυχές που αναδείχθηκαν με την παρούσα μένει να αναδειχθούν και στην πράξη καθώς το metaverse φαίνεται να είναι μια πολλά υποσχόμενη τεχνολογία, η οποία αναπτύσσεται προοδευτικά και προκειμένου να αποδώσει τους καρπούς της, θα πρέπει πρωτίστως να παραμετροποιηθεί σε όλα τα επίπεδα προκειμένου να διαχειριστεί με τον καλύτερο δυνατό τρόπο τις ευαίσθητες ισορροπίες που δημιουργούνται και συνεχώς διαμορφώνονται μεταξύ των παρόχων/πλατφορμών του metaverse, των άβαταρ, καθώς και των φυσικών προσώπων πίσω από τα άβαταρ. Πιο συγκεκριμένα η πάλη αυτών των ισορροπιών θα αφορά την ύπαρξη μιας άρτια δομημένης τεχνολογίας σε τεχνικό και νομικό επίπεδο, η οποία θα καθιστά πιο ομαλή τη μετάβαση από τον πραγματικό στον εικονικό κόσμο και θα προσαρμόζεται επαρκώς στις εκάστοτε νέες περιπτώσεις και προκλήσεις που θα συναντά.

[350] Pietro, Di R., and Cresci, S. (2021), ό.π., σελ. 286

8. ΒΙΒΛΙΟΓΡΑΦΙΑ

8.1. Ελληνική

Συγγράμματα

Γιαννακόπουλος, Κ. (2022) *Ο νεοφεουδαρχικός συνταγματισμός*, Αθήνα – Θεσσαλονίκη: Εκδόσεις Σάκκουλα

Ιγγλεζάκης, Ι. (2022) *Το δίκαιο της ψηφιακής οικονομίας*, Αθήνα – Θεσσαλονίκη: Εκδόσεις Σάκκουλα

Σπηλιόπουλος, Ο. (2020) *Οικονομικό δίκαιο της Ευρωπαϊκής Ένωσης*, Αθήνα – Θεσσαλονίκη: Εκδόσεις Σάκκουλα

Διπλωματικές Εργασίες

Αποστολάτου, Χ. (2022) *Η χρήση της Meta ως μέσο προβολής marketing*, Πανεπιστήμιο Μακεδονίας, Δημοκρίτειο Πανεπιστήμιο Θράκης. Διαθέσιμο σε: https://dspace.lib.uom.gr/bitstream/2159/27802/3/ApostolatouCharikleiaMcs2022.pdf (Τελευταία πρόσβαση: 06.06.2023)

Άρθρα

Θεοδωράκης, Ν. και Καλογεράκης, Γ. (2019) 'Blockchain: εφαρμογές, προοπτικές και προκλήσεις για το ελληνικό νομικό σύστημα – Ιδίως οι εφαρμογές του στις έννομες σχέσεις ιδιωτικού δικαίου', *ΔΙΤΕ (π. ΔΙΜΕΕ)*, 16 (1). Διαθέσιμο σε: https://www.academia.edu/40377994/%CE%9A%CE%B1%CE%BB%CE%BF%CE%B3%CE%B5%CF%81%CE%AC%CE%BA%CE%B7%CF%82_%CE%98%CE%B5%CE%BF%CE%B4%CF%89%CF%81%CE%AC%CE%BA%CE%B7%CF%82_Blockchain_%CE%B5%CF%86%CE%B1%CF%81%CE%BC%CE%BF%CE%B3%CE%AD%CF%82_%CF%80%CF%81%CE%BF%CE%BF%CF%80%CF%84%CE%B9%CE%BA%CE%AD%CF%82_%CE%BA%CE%B1%CE%B9_%CF%80%CF%81%CE%BF%CE%BA%CE%BB%CE%AE%CF%83%CE%B5%CE%B9%CF%82_%CE%B3%CE%B9%CE%B1_%CF%84%CE%BF_%CE%B5%CE%BB%CE%BB%CE%B7%CE%BD%CE%B9%CE%B

A%CF%8C_%CE%BD%CE%BF%CE%BC%CE%B9%CE%BA%CF%8C_%CF%83%CF%8D%CF%83%CF%84%CE%B7%CE%BC%CE%B1_%CE%94i%CE%9C%CE%95%CE%95_2019_%CF%83_5%CE%B5%CF%80 (Τελευταία πρόσβαση: 10.06.2023)

Καρδαμάκη, Α. (2022), 'Εικονικοί Κόσμοι, Metaverse και Προστασία Δεδομένων Προσωπικού Χαρακτήρα', *Επιθεώρηση Δικαίου Πληροφορικής*, Τόμ. 3, Αρ. 1. Διαθέσιμο σε: https://ejournals.lib.auth.gr/infolawj/article/view/8907 (Τελευταία πρόσβαση: 15.05.2023)

Κόκιου, Β. (2022) 'Νομικά ζητήματα στον χώρο του Metaverse'. Διαθέσιμο σε: https://www.capital.gr/me-apopsi/3635339/nomika-zitimata-ston-xoro-tou-metaverse/ (Τελευταία πρόσβαση: 13.05.2023)

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

Χιόνη, Γ. (2022) 'Δίκαιο και Μετασύμπαν (Metaverse): Προκλήσεις και νομικά ζητήματα Ι'. Διαθέσιμο σε: https://www.lawspot.gr/nomika-blogs/georgia_hioni/dikaio-kai-metasympan-metaverse-prokliseis-kai-nomika-zitimata-i (Τελευταία πρόσβαση: 13.05.2023)

Χιόνη, Γ. (2022) 'Δίκαιο και Μετασύμπαν (ΙΙ): Το δίκαιο των avatar'. Διαθέσιμο σε: https://www.lawspot.gr/nomika-blogs/georgia_hioni/dikaio-kai-metasympan-ii-dikaio-ton-avatar (Τελευταία πρόσβαση: 11.06.2023)

8.2. Ξενόγλωσση

Συγγράμματα

Boni, M. (2023), *Ethical challenges related to the Metaverse development -hypothesis*, *IntechOpen*. Διαθέσιμο σε: https://www.intechopen.com/online-first/1131705 (Τελευταία πρόσβαση: 16.06.2023)

Άρθρα

Angeles, J. (2022). 'The EU legal obligations of very large platforms providing digital services in the age of the metaverse'. *Cuadernos de Derecho Transnacional*, 14(2), 294-318. Διαθέσιμο σε: CUADERNOS DE DERECHO TRANSNACIONAL (uc3m.es) (Τελευταία πρόσβαση: 16.06.2023)

Ara, T. et al., (2022), 'Exploring the metaverse: What laws will apply?'. Διαθέσιμο σε: https://www.dlapiper.com/en/insights/publications/2022/02/exploring-the-metaverse (Τελευταία πρόσβαση: 16.06.2023)

Arzt, M. and Weingarden, G. (2022), 'Metaverse and privacy'. Διαθέσιμο σε: https://iapp.org/news/a/metaverse-and-privacy-2/ (Τελευταία πρόσβαση: 14.06.2023)

Bale, A.S. et al. (2022) 'A Comprehensive Study on Metaverse and Its Impacts on Humans'. *Advances in Human-Computer Interaction*, vol. 2022, Article ID 3247060. Διαθέσιμο σε: https://www.hindawi.com/journals/ahci/2022/3247060/ (Τελευταία πρόσβαση: 16.05.2023)

Bravo, A. (2023). 'MDE#07 The Digital Markets Act'. Διαθέσιμο σε: https://www.metaversethics.org/p/mde07-the-digital-markets-act (Τελευταία πρόσβαση: 17.06.2023)

Buck, L. and McDonell, R. (2022) 'Security and Privacy in the Metaverse: The Threat of the Digital Human', *CHI EA '22, April 29 - May 5, 2022*, New Orleans, LA, USA. Διαθέσιμο σε: https://www.researchgate.net/publication/360476399_Security_and_Privacy_in_the_Metaverse_The_Threat_of_the_Digital_Human (Τελευταία πρόσβαση: 13.06.2023)

Cheng, R., Wu, N., Chen S. and Han, B. (2022) "Will Metaverse Be NextG Internet? Vision, Hype, and Reality," in *IEEE Network*, vol. 36, no. 5, pp. 197-204, September/October 2022. Διαθέσιμο σε: https://ieeexplore.ieee.org/document/9877927 (Τελευταία πρόσβαση: 16.05.2023)

Cheng S., Zhang Y., Li X., et al., (2022) 'Roadmap toward the metaverse: An AI perspective' *The Innovation*, 3(5), 100293. Διαθέσιμο σε: https://www.cell.com/the-innovation/pdf/S2666-6758(22)00089-3.pdf (Τελευταία πρόσβαση: 16.05.2023)

Cheong, B.C. (2022) 'Avatars in the metaverse: potential legal issues and remedies'. *Int. Cybersecur. Law Rev.* **3**, 467–494. Διαθέσιμο σε: https://link.springer.com/article/10.1365/s43439-022-00056-9#citeas (Τελευταία πρόσβαση: 13.06.2023)

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)*, Bologna, Italy, pp. 272-277. Διαθέσιμο σε: https://arxiv.org/pdf/2204.01480.pdf (Τελευταία πρόσβαση: 17.05.2023)

Floridi, L. (2022), 'Metaverse: A Matter of Experience' *Philosophy & Technology*, 35, 73. Διαθέσιμο σε: https://doi.org/10.1007/s13347-022-00568-6 (Τελευταία πρόσβαση: 06.06.2023)

Gordon, M. (2022), 'The Metaverse: What are the legal implications?', *Clifford Chance*. Διαθέσιμο σε: https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2022/02/the-metaverse-what-are-the-legal-implications.pdf (Τελευταία πρόσβαση: 17.05.2023)

Gorichanaz, T. (2022), 'Being at home in the metaverse? Prospectus for a social imaginary', *AI and Ethics* 3, pp. 647–658. Διαθέσιμο σε: https://link.springer.com/article/10.1007/s43681-022-00198-w (Τελευταία πρόσβαση: 17.05.2023)

Mackenzie, R. et al., (2022), 'Legal issues (part 2) Managing antitrust & competition risk', *The Reed Smith Guide to the Metaverse - 2nd Edition*. Διαθέσιμο σε: https://www.reedsmith.com/en/perspectives/metaverse/2022/08/managing-antitrust-and-competition-risk (Τελευταία πρόσβαση: 16.06.2023)

Megale, L. (2022). '(Meta)verse as the Next Escaper from Competition Public Enforcement'. *Market and Competition Law Review*, 6(2), 15-50. Διαθέσιμο σε: https://revistas.ucp.pt/index.php/mclawreview/article/view/11715 (Τελευταία πρόσβαση: 17.06.2023)

Murphy, S. et aI., (2021) 'The Metaverse: The evolution of a universal digital platform'. Διαθέσιμο σε: https://www.nortonrosefulbright.com/en-gr/knowledge/publications/5cd471a1/the-metaverse-the-evolution-of-a-universal-digital-platform (Τελευταία πρόσβαση: 11.06.2023)

Petrányi, D., Horváth, K. and Domokos, M. (2022) 'Legal issues in the metaverse / Part 1 - Introduction to the metaverse'. Διαθέσιμο σε: https://cms-lawnow.com/en/ealerts/2022/07/legal-issues-in-the-metaverse-part-1-introduction-to-the-metaverse (Τελευταία πρόσβαση: 11.06.2023)

Petrányi, D., Horváth, K. and Domokos, M. (2022) 'Part 3 - Data protection challenges, the importance of cybersecurity, advertising regulation in the metaverse'. Διαθέσιμο σε: https://cms.law/en/int/publication/legal-issues-in-the-metaverse/part-3-data-protection-challenges-the-importance-of-cybersecurity-advertising-regulation-in-the-metaverse (Τελευταία πρόσβαση: 14.06.2023)

Pietro, Di 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)*, Atlanta, GA, USA, pp. 281-288. Διαθέσιμο σε: https://ieeexplore.ieee.org/document/9750221 (Τελευταία πρόσβαση: 10.06.2023)

Plechatá, A., Makransky, G. and Böhm, R. (2022) 'Can extended reality in the metaverse revolutionise health communication?', *npj Digital Medicine*, 5, 132. Διαθέσιμο σε: https://doi.org/10.1038/s41746-022-00682-x (Τελευταία πρόσβαση: 11.06.2023)

Sampaio, G. and Vaz M.C. (2022), 'Civil liability in the Metaverse'. Διαθέσιμο σε: https://www.bmalaw.com.br/en-US/pi/conteudo/contencioso-e-arbitragem/civil-liability-in-the-metaverse (Τελευταία πρόσβαση: 14.06.2023)

Stolton, S. (2022), 'Vestager: Metaverse poses new competition challenges', *Politico*, 18 January. Διαθέσιμο σε: https://www.politico.eu/article/metaverse-new-competition-challenges-margrethe-vestager/ (Τελευταία πρόσβαση: 14.06.2023)

Warin, C. and Reinhardt, D. (2022). 'Vision: Usable Privacy for XR in the Era of the Metaverse'. *2022 European Symposium on Usable Security (EuroUSEC 2022)*, σελ.111-116. Διαθέσιμο σε: https://dl.acm.org/doi/pdf/10.1145/3549015.3554212?casa_token=2rhHWgG3ZyYAAAAA:MZp5BdPuA2mm7fLhBvPGsjbNqVWWb55YfXu_nWw_R4rMADGf0O3l2c_S-5RwTGifV4A7u30jrIAS (Τελευταία πρόσβαση: 17.05.2023)

Μελέτες

Dwivedi, K. Y. et al. (2022), *Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy*, International Journal of Information Management, Volume 66. Διαθέσιμο σε: https://www.sciencedirect.com/science/article/pii/S0268401222000767 (Τελευταία πρόσβαση: 10.06.2023)

Europol (2022), *Policing in the metaverse: what law enforcement needs to know, an observatory report from the Europol Innovation Lab*, Luxembourg: Publications Office of the European Union.

Διαθέσιμο σε: https://www.europol.europa.eu/cms/sites/default/files/documents/Policing%20in%20the%20metaverse%20-%20what%20law%20enforcement%20needs%20to%20know.pdf (Τελευταία πρόσβαση: 13.06.2023)

Madiega, T., Car, P. et aI., (2022), *Metaverse Opportunities, risks and policy implications,* European Parliamentary Research Service (EPRS). Διαθέσιμο σε: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733557 (Τελευταία πρόσβαση: 20.05.2023)

Maciejewski, M. (2023), *Metaverse,* Study for the JURI Committee, Policy Department for Citizens' Rights and Constitutional Affairs, European Parliament, Brussels. Διαθέσιμο σε: https://www.europarl.europa.eu/RegData/etudes/STUD/2023/751222/IPOL_STU(2023)751222_EN.pdf (Τελευταία πρόσβαση: 03.07.2023)

Nair, V., Garido, M. G. and Song, D. (2022), *Exploring the Unprecedented Privacy Risks of the Metaverse.* Διαθέσιμο σε: https://arxiv.org/abs/2207.13176 (Τελευταία πρόσβαση: 14.06.2023)

Nair, V., Garido, M. G. and Song, D. (2022), *Going Incognito in the Metaverse.* Διαθέσιμο σε: https://arxiv.org/abs/2208.05604 (Τελευταία πρόσβαση: 13.06.2023)

Zhu, L. (2022), *The Metaverse: Concepts and Issues for Congress,* CRS Reports. Διαθέσιμο σε: https://crsreports.congress.gov/product/pdf/R/R47224 (Τελευταία πρόσβαση: 16.05.2023)

8.3. Ιστότοποι

Ευρωπαϊκή Επιτροπή (2023), *Εικονικοί Κόσμοι κατάλληλοι για τους ανθρώπους.* Διαθέσιμο σε: https://digital-strategy.ec.europa.eu/el/policies/virtual-worlds (Τελευταία πρόσβαση: 14.07.2023)

Ευρωπαϊκή Επιτροπή (2023), *Ερωτήσεις και απαντήσεις: Πράξη για τις ψηφιακές αγορές: Διασφάλιση δίκαιων και ανοικτών ψηφιακών αγορών.* Διαθέσιμο σε: https://ec.europa.eu/commission/presscorner/detail/el/QANDA_20_2349 (Τελευταία πρόσβαση: 17.06.2023)

Ευρωπαϊκή Επιτροπή (2023), *Ερωτήσεις και απαντήσεις: πράξη για τις ψηφιακές υπηρεσίες.* Διαθέσιμο σε: https://ec.europa.eu/commission/presscorner/detail/el/QANDA_20_2348 (Τελευταία πρόσβαση: 16.06.2023)

Ευρωπαϊκή Επιτροπή (2023), *Πράξη για τις ψηφιακές υπηρεσίες: διασφάλιση ενός ασφαλούς και υπεύθυνου διαδικτυακού περιβάλλοντος.* Διαθέσιμο σε: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_el (Τελευταία πρόσβαση: 16.06.2023)

Ευρωπαϊκή Επιτροπή (2023), *Πράξη για τις ψηφιακές υπηρεσίες: η Επιτροπή ορίζει τις πρώτες πολύ μεγάλες επιγραμμικές πλατφόρμες και μηχανές αναζήτησης.* Διαθέσιμο σε: https://ec.europa.eu/commission/presscorner/detail/el/IP_23_2413 (Τελευταία πρόσβαση: 16.06.2023)

Ευρωπαϊκή Επιτροπή (2023), *Προς την επόμενη τεχνολογική μετάβαση: η Επιτροπή παρουσιάζει στρατηγική της ΕΕ για την ανάληψη ηγετικής θέσης στο Web 4.0 και στους εικονικούς κόσμους.* Διαθέσιμο σε: https://ec.europa.eu/commission/presscorner/detail/el/ip_23_3718 (Τελευταία πρόσβαση: 14.07.2023)

Ευρωπαϊκή Επιτροπή, *Μια Ευρώπη έτοιμη για την ψηφιακή εποχή: νέοι κανόνες για τις διαδικτυακές πλατφόρμες.* Διαθέσιμο σε: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment/europe-fit-digital-age-new-online-rules-platforms_el (Τελευταία πρόσβαση: 16.06.2023)

Ευρωπαϊκή Επιτροπή (2023), *Keynote delivered by EVP Vestager for the Keystone Conference: A Triple Shift for competition policy.* Διαθέσιμο σε: https://ec.europa.eu/commission/presscorner/detail/el/SPEECH_23_1342 (Τελευταία πρόσβαση: 16.06.2023)

Συμβουλευτική Επιτροπή Βιομηχανικών Μεταλλαγών (2023), *Πρωτοβουλία για τους εικονικούς κόσμους, όπως το μετασύμπαν (metaverse).* Διαθέσιμο σε: https://eur-

lex.europa.eu/legal-content/EL/TXT/HTML/?uri=PI_EESC:EESC-2023-00888-AS (Τελευταία πρόσβαση: 16.06.2023)

Συμβούλιο της ΕΕ (2021), *Ό,τι είναι παράνομο εκτός διαδικτύου θα πρέπει να είναι παράνομο και στο διαδίκτυο: Καθορισμός της θέσης του Συμβουλίου σχετικά με την πράξη για τις ψηφιακές υπηρεσίες.* Διαθέσιμο σε: https://www.consilium.europa.eu/el/press/press-releases/2021/11/25/what-is-illegal-offline-should-be-illegal-online-council-agrees-on-position-on-the-digital-services-act/ (Τελευταία πρόσβαση: 16.06.2023)

Council of the European Union (2022), Metaverse – Virtual World, Real Challenges. Διαθέσιμο σε: https://www.consilium.europa.eu/media/54987/metaverse-paper-9-march-2022.pdf (Τελευταία πρόσβαση: 17.06.2023)

8.4. Νομοθετικά κείμενα

Ενοποιημένη απόδοση της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης Πρωτόκολλα Παραρτήματα της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης Δηλώσεις οι οποίες προσαρτώνται στην τελική πράξη της διακυβερνητικής διάσκεψη η οποία υιοθέτησε τη Συνθήκη της Λισσαβώνας που υπογράφηκε στις 13 Δεκεμβρίου 2007. Διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A12016ME%2FTXT (Τελευταία πρόσβαση: 16.06.2023)

Κανονισμός (ΕΕ) 2023/1114 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 31ης Μαΐου 2023 για τις αγορές κρυπτοστοιχείων και για την τροποποίηση των κανονισμών (ΕΕ) αριθ. 1093/2010 και (ΕΕ) αριθ. 1095/2010 και των οδηγιών 2013/36/ΕΕ και (ΕΕ) 2019/1937. Διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:32023R1114 (Τελευταία πρόσβαση: 17.06.2023)

Κανονισμός (ΕΕ) 2023/988 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 10ης Μαΐου 2023 για τη γενική ασφάλεια των προϊόντων, την τροποποίηση του κανονισμού (ΕΕ) αριθ. 1025/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και της οδηγίας (ΕΕ) 2020/1828 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, και την κατάργηση της οδηγίας 2001/95/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και της οδηγίας 87/357/ΕΟΚ του Συμβουλίου. Διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32023R0988 (Τελευταία πρόσβαση: 16.06.2023)

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). Διαθέσιμο σε https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:32022R2065 (Τελευταία πρόσβαση: 11.06.2023)

Κανονισμός (ΕΕ) 2022/1925 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 14ης Σεπτεμβρίου 2022 σχετικά με διεκδικήσιμες και δίκαιες αγορές στον ψηφιακό τομέα και για την τροποποίηση των οδηγιών (ΕΕ) 2019/1937 και (ΕΕ) 2020/1828 (Πράξη για τις Ψηφιακές Αγορές). Διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/ELL/TXT/?uri=uriserv%3AOJ.L_.2022.265.01.0001.01.ELL&toc=OJ%3AL%3A2022%3A265%3ATOC (Τελευταία πρόσβαση: 11.06.2023)

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). Διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32016R0679 (Τελευταία πρόσβαση: 13.06.2023)

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). Διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32022L2555 (Τελευταία πρόσβαση: 13.06.2023)

Οδηγία (ΕΕ) 2019/770 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 20ής Μαΐου 2019, σχετικά με ορισμένες πτυχές που αφορούν τις συμβάσεις για την προμήθεια ψηφιακού περιεχομένου και ψηφιακών υπηρεσιών. Διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32019L0770 Τελευταία πρόσβαση: 14.07.2023)

Οδηγία (ΕΕ) 2019/771 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 20ής Μαΐου 2019, σχετικά με ορισμένες πτυχές που αφορούν τις συμβάσεις για τις πωλήσεις αγαθών, την τροποποίηση του κανονισμού (ΕΕ) 2017/2394 και της οδηγίας 2009/22/ΕΚ, και την κατάργηση της

οδηγίας 1999/44/ΕΚ. Διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/el/TXT/?uri=CELEX%3A32019L0771 (Τελευταία πρόσβαση: 14.07.2023)

Οδηγία (ΕΕ) 2018/843 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 30ής Μαΐου 2018, για την τροποποίηση της οδηγίας (ΕΕ) 2015/849 σχετικά με την πρόληψη της χρησιμοποίησης του χρηματοπιστωτικού συστήματος για τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες ή για τη χρηματοδότηση της τρομοκρατίας, και για την τροποποίηση των οδηγιών 2009/138/ΕΚ και 2013/36/ΕΕ (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ). Διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32018L0843 (Τελευταία πρόσβαση: 13.06.2023)

Οδηγία 2000/31/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 8ης Ιουνίου 2000 για ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά («οδηγία για το ηλεκτρονικό εμπόριο»). Διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=celex:32000L0031 (Τελευταία πρόσβαση: 16.06.2023)

Πρόταση Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με οριζόντιες απαιτήσεις κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία και με την τροποποίηση του κανονισμού (ΕΕ) 2019/1020, Βρυξέλλες, 15.9.2022, COM(2022) 454 final, 2022/0272(COD). Διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:52022PC0454 (Τελευταία πρόσβαση: 13.06.2023)

Πρόταση Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τη θέσπιση κανόνων με σκοπό την πρόληψη και την καταπολέμηση της σεξουαλικής κακοποίησης παιδιών, Βρυξέλλες, 11.5.2022, COM(2022) 209 final, 2022/0155(COD). Διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:52022PC0209 (Τελευταία πρόσβαση: 13.06.2023)

Πρόταση Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τη θέσπιση εναρμονισμένων κανόνων σχετικά με την τεχνητή νοημοσύνη (Πράξη για την Τεχνητή Νοημοσύνη – AI Act) και για την τροποποίηση ορισμένων νομοθετημάτων πράξεων της Ένωσης, Βρυξέλλες 21.04.2021, COM(2021) 206 final, 2021/0106(COD). Διαθέσιμο σε https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A52021PC0206 (Τελευταία πρόσβαση: 19.05.2023)

Πρόταση Οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προσαρμογή των κανόνων περί εξωσυμβατικής αστικής ευθύνης στην τεχνητή νοημοσύνη (οδηγία περί ευθύνης για την ΤΝ), Βρυξέλλες, 28.9.2022, COM(2022) 496 final, 2022/0303(COD). Διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:52022PC0496 (Τελευταία πρόσβαση: 13.06.2023)